¿TU LINUX ESTÁ TOTALMENTE SEGURO?



LA MEJOR REVISTA TÉCNICA EN ESPAÑOL #46

Eligiendo la VIDEOCÁMARA perfecta

SEGURIDAD

WIRELESS

TODO LO QUE TENES QUE SABER

Implementación de **ADSL**

VOIP: Inicio, objetivos y requerimientos

INNOVADORES ICT



CONOZCA A LOS **MEJORES**

Steve Jobs
Creador de Apple

SEGURIDAD
Las predicciones para 2008

WWW.NEXWEB.COM.AR

NEX IT SPECIALIST - STAFF

DIRECTOR
- Dr. Carlos Osvaldo Rodríguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

COORDINACIÓN EDITORIAL
- María Delia Cardenal
- Carlos Rodríguez

SENIOR SECURITY EDITOR
- Carlos Vaughn O'Connor

DEPARTAMENTO COMERCIAL
- Ignacio Tellería
itelleria@nexweb.com.ar

EDITORES TÉCNICOS
- Thomas Hughes
- Ariel Cortéz
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- Florencia Mangiantini
- Carlos Rodríguez Bontempi
- Federico Arena
- Matías Ruiz

DISTRIBUCIÓN
distribucion@nexweb.com.ar

SUSCRIPCIONES
suscripciones@nexweb.com.ar

PREIMPRESIÓN E IMPRESIÓN
Talleres gráficos VALDEZ
Loyola 1581. Cap. Fed.
Tel 4854-3437

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Huesca Distribuidora de Publicaciones S.A. Aristóbulo del Valle 1556/58. C1295ADH - Capital Federal Argentina. (www.distribuidorahuesca.com.ar)
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1
C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar





En el exigente, dinámico y desafiante mundo de las Tecnologías de la Información y Comunicación conocer cuáles son las habilidades y conocimientos más demandados por la industria puede ser la vital diferencia entre conseguir un trabajo que nos ayude a pagar las cuentas o desarrollar una carrera exitosa y apasionante.

Organizaciones como CompTIA (Computing Technology Industry Association) o medios como Network World han elaborado listas con las demandas más requeridas y por ende mejor pagas de la industria. Les presentamos un resumen que puede ser útil a la hora de elegir o reorientar nuestro perfil profesional.

1. Wireless
La proliferación de dispositivos de conexión inalámbrica y la necesidad de los usuarios de conectarse en cualquier momento y lugar hacen que las competencias en movilidad inalámbrica sean cada vez más necesarias y valoradas.

2. Virtualización
Es el futuro del Data Center y de las TICs en general y como se trata de un ámbito relativamente nuevo la industria requiere con urgencia de expertos en el tema.

3. Seguridad
Dado que la información es el activo más importante de las empresas en estos tiempos, ser un experto en seguridad, garantiza infinitas y atractivas posibilidades.

4. Networking
Con el crecimiento y la complejidad de las redes, las habilidades para diseñarlas y administrarlas resultan un activo muy cotizado. VoIP o IPv6 son algunas de las tecnologías que los Networks deberán dominar en poco tiempo.

5. Application delivery
Con redes más complejas y sofisticadas, que una firma cuente con expertos en Aplicación de entrega puede significar mayor satisfacción para los usuarios y una gran disminución de costos.

6. Web 2,0
AJAX, .NET y Java, otras habilidades de desarrollo, son tecnologías fundamentales para que las empresas puedan utilizar las útiles herramientas colaborativas.

7. IT Business Análisis
Ser capaz de evaluar inversiones, planificación estratégica y beneficios resulta fundamental para todos los recursos que trabajan en IT.

8. Gestión de bases de datos
SQL, MySQL y Oracle son algunos de los conocimientos más requeridos para la gestión de bases de datos, un rubro con demanda en todas las industrias de la economía.

9. Inteligencia de negocios/Data Mining
Relacionado con los ítems anteriores, la habilidad para analizar los datos almacenados ocupa un lugar cada vez más central en las empresas. No solo recolectar datos, sino y sobre todo analizarlos extraer conclusiones y aplicarlas en la gestión del negocio.

10. La carta ganadora
Como las redes y sistemas son cada vez más complejos y entrelazados entre si, las empresas esperan que el personal de IT posea conocimientos y expertise en diversas áreas y que sea capaz de poder integrarlo de manera eficiente. Las fronteras entre sistemas, aplicaciones y tecnologías se van borrando paulatinamente y el personal IT debe estar capacitado para adaptarse al nuevo escenario. ●

LOS H

La confiabilidad que necesita

EDICIÓN ESPECIAL



Megatone adoptó la plataforma más confiable para agilizar sus procesos de negocio

Luego de diversas pruebas, la plataforma Microsoft demostró ser más segura. **Pág. 15**

Al migrar de Linux a Windows Server, la empresa conectó las sucursales incrementando la productividad de todos sus empleados y del área de Sistemas.

Megatone, la mayor cadena de comercialización de artículos del hogar, operaba con servidores y escritorios de Linux, lo que requería tiempo y esfuerzo. La estructura informática creció por lo que la administración sobre este tipo de plataforma se hizo demasiado compleja.

Además, el uso de Linux en sus estaciones de trabajo presentaba limitaciones de compatibilidad y en el manejo de planillas de cálculo complejas. "Hicimos un estudio analizando lo que este producto exigía a nivel de hardware y el costo de licencias a tres años y resultaba demasiado costoso. Eso, sumado a que no tuviera las prestaciones requeridas, nos impulsó a abandonarlo", comenta Pablo Gracia, gerente de Megatone. Teniendo en cuenta las nuevas y cambiantes necesidades del negocio, la empresa decidió emprender la renovación tecnológica de sus sistemas con Microsoft Exchange Server 2003, SQL Server 2005 y Microsoft Virtual Server 2005, apuntando a una consolidación del 50% de los servidores. "Los buenos resultados que estamos apreciando con la virtualización nos permiten concentrar los esfuerzos del área de Sistemas, lo que redunda en más eficiencia operativa. Megatone completará la migración de todos sus servidores y sus 2500 escritorios Linux a Windows XP y Microsoft Office 2003. Incorporaremos nuevas aplicaciones desarrolladas con .NET", agrega Gabriel Alessandria, gerente de Megatone.

Por su parte, Oscar Finochietti, gerente de la firma, dice que es clave agilizar el flujo de información y favorecer la colaboración entre los empleados. "Somos muchos y estamos dispersos, pero necesitamos intercambiar permanentemente documentación. La solución que nos proveen SharePoint y Exchange Server junto a Outlook es muy potente", sostiene el ejecutivo. "Estamos montando una plataforma integrada, confiable y fácil de administrar que cubre todas nuestras necesidades", asegura Gracia.

Continúa en Pág. 3.

ECHOS

para tomar sus decisiones

Para conocer más sobre este y otros casos visite www.microsoft.com/argentina/hechos o llame al 0800-999-4617

FOTO: P. GONZALEZ



En primera persona

"En un momento de mucho crecimiento se empezó a hacer más compleja la administración de la infraestructura en Linux. Llevaba mucho esfuerzo y tiempo de nuestro equipo."

Gabriel Alessandria,
Gerente de Megatone.

Red de negocios

Megatone, la red de artículos para el hogar más grande del país, tiene 160 servidores en tres centros de cómputos y más de 2500 puestos de trabajo en 200 sucursales. Emplea a 7000 personas y cuenta con nueve centros de operaciones logísticas y dos fábricas de su propia marca de PCs. **Pág. 7**

Resultados tangibles

Con la migración de sus PCs y servidores a la plataforma Microsoft, con Windows Server System, Windows XP y Microsoft Office, Megatone consolidó el 50% de servidores, facilitó la administración de los sistemas y el acceso a información en cualquier momento y desde cualquier lugar con seguridad a través de VPN. **Pág. 15**

La interoperabilidad

NEX IT

LA MEJOR REVISTA TECNICA EN ESPAÑOL

NOTA DE TAPA



SUMARIO - EDICIÓN #46

Snoop Update 2008

A mediados de abril, como hace ya tres años, se realizó el Update 2008, el evento para desarrolladores más grande de la región, organizado por Snoop Consulting, una de las consultoras de desarrollo e implementaciones de soluciones de nuestro país más importantes.
Durante toda una jornada se dictaron diferentes charlas sobre las nuevas tendencias y los últimos avances en la industria del software local, y se debatió sobre Web 2.0, programación Multicore, bpi OpenESB, Seaside, Agile, Ruby, .Net, SaaS, Google Gears y Adobe Air.
Con respecto a los oradores, el encuentro contó con la participación de Emmanuel Bernard (Core Developer en JBoss), Sang Shin (arquitecto de tecnología y consultor de Sun Microsystems) y Arzhan Kinzhalin (del centro de desarrollo de software de Intel Argentina).

"Snoop organiza este evento como parte de la responsabilidad que tiene como empresa", señaló Gustavo Guaragna, CEO de Snoop Consulting. "Es además, nuestra forma de dar las gracias a la comunidad que nos hizo crecer. Queremos que sea el evento para desarrolladores más importante del año".

Como novedad, este año se implementaron los "F2F" (Face to Face), grupos informales de discusión cara a cara con los keynotes speakers. Estos grupos consisten de un reducido número de personas con el objetivo de generar debate sobre un tema específico.
Por otra parte, también se realizó el Update 4CIOs, un encuentro pensado para debatir sobre la tecnología y los negocios.

"El UPDATE 4CIOs estuvo dirigido a los responsables de evaluar el impacto de la tecnología en sus organizaciones, de acuerdo con la realidad regional", indicó Guaragna. *"A su vez, este encuentro brindó la posibilidad de realizar networking con los referentes de la industria"*, agregó.

En esta ocasión, Leonardo Schvarstein, ingeniero industrial y psicólogo social, dio una charla sobre gestión del cambio; y Jorge Forteza, Chairman del Consejo de Administración de la Universidad de San Andrés en Buenos Aires, habló sobre la cadena de valor.
A su vez, hubo un panel sobre tendencias tecnológicas, del que participaron Alejandro de León, Presidente de Oracle para Argentina, Uruguay, Paraguay y Bolivia; Gustavo Ripoll, Gerente General de Microsoft en Argentina, y Presidente del Instituto para el Desarrollo Empresarial de la Argentina (IDEA); y Alejandro Raffaele, Country Manager de Sun Microsystems Argentina.





Junio		
5 y 6	**InfoSecurity Buenos Aires** Hotel Sheraton y Crucero Galileo	www.infosecurityonline.org
10	**IDC Argentina Business Intelligence 2.0 Conference** - A confirmar -	www.idclatin.com/argentina/
Julio		
3	**IDC Argentina Business Mobility & Convergence Conference 2008** - A confirmar -	www.idclatin.com/argentina/

EMPRESA EFICIENTE GARANTIZADA

CONSERVACIÓN DE LA ENERGÍA
Aproveche los beneficios de un sistema de energía eficiente dimensionando adecuadamente su infraestructura, y pagará sólo lo que necesite.

ENFRIAMIENTO ESTRECHAMENTE ACOPLADO
Logre mayor eficiencia térmica con la arquitectura de refrigeración InRow™. Reduciendo la distancia a recorrer por el aire frío (de 15 m a 1,5 m), se elimina la mezcla del aire extraído caliente con el aire frío de la sala, y se vuelve viable un sistema de enfriamiento de precisión más dirigido.

ADMINISTRACIÓN DE LA CAPACIDAD
Administre sus sistemas con máxima eficiencia mediante el software inteligente e integrado para administración de la capacidad, con datos exactos y en tiempo real sobre dónde refrigerar y a qué suministrar energía.

Presentamos Efficient Enterprise™: más energía, más control, más ganancias.

¿Acaso su sistema actual puede ofrecerle lo mismo?

Los potentes sistemas legados funcionan bien cuando se trata de enfriar salas completas, pero los altísimos costos de la energía hacen que elegirlos resulte irresponsable desde el punto de vista físico, y el sobredimensionamiento inherente a su diseño los vuelve inadecuados para enfrentar los desafíos actuales en materia de alta densidad. Para un problema simple, una solución simple. Reduzca sus costos de energía y refrigeración, y utilice los ahorros para comprar los equipos informáticos que necesita. Según la firma Gartner Research, el 50% de los centros de datos construidos antes de 2002 serán obsoletos para 2008 debido a su deficiente capacidad para suministrar energía y refrigeración. El problema más importante que enfrentan los gerentes de data centers actualmente se relaciona con la energía y refrigeración.

CONTENCIÓN DEL CALOR
Eleve sus niveles de eficiencia con el esquema de refrigeración conteniendo el calor y eliminando la costosa contaminación cruzada de temperaturas. Nuestro sistema de contención de pasillo caliente reduce los costos operativos hasta un 50% respecto de los enfoques basados en sistemas legados.



Efficient Enterprise™ de APC-MGE.

Esta solución de APC-MGE. para empresas eficientes le permite aprovechar sus recursos al máximo. Escalabilidad modular, para que sólo pague por lo que use, administración de la capacidad que le permite saber dónde ubicar él próximo servidor, y sistemas por hilera y de contención de calor dedicados que aumentan la predecibilidad de los niveles térmicos y de refrigeración. La arquitectura Efficient Enterprise le hace ganar dinero ayudándolo a eliminar los gastos excesivos. Por ejemplo, con sólo pasar de un esquema de refrigeración para toda la sala a uno por hilera, ahorrará en promedio 35% en costos de electricidad.

Nuestro sistema le devuelve su dinero

Ya sea que construya un centro de datos nuevo o analice la eficiencia de sistemas existentes, lo primero que debe saber es dónde está parado. Aproveche el servicio online de Auditoría de Efficient Enterprise™ para saber cómo obtener beneficios con un sistema inteligente, integrado y eficiente: más energía, más control, más ganancias.





¿Qué grado de eficiencia tiene su sistema corporativo?

Sepa exactamente dónde está parado: aproveche el servicio de Auditoría de la eficiencia de la empresa hoy mismo.

Visite www.apc.com/promo Código 63553d • Llame al 0-800-222-3232

nexmedia.com.ar

NOTICIAS

¿Hacia donde va Yahoo?

Las presiones de accionistas y el mercado financiero hicieron que Yang se replantee el rechazo a Microsoft, mientras intenta conducir sin rumbo fijo los destinos del gigante de Internet.
Parece cerrarse la larga historia entorno a la oferta de Microsoft para comprar Yahoo.

TIPS

5 claves para mantenerse a salvo del spam

Cinco tips para evitar el correo basura sin dejar de acceder a todo lo que le interesa en línea.
1) Crear una dirección mailinator.com
Mailinator es un servicio gratuito que permite crear direcciones de correo electrónico temporal sobre la marcha cuando usted llena formularios en línea...

HARDWARE

Intel vs. AMD: La batalla por los cuatro núcleos

Mientras Intel bate records de ventas con sus Quad Core, AMD se prepara para dar pelea con el relanzamiento de sus procesadores de cuatro núcleos nativos.

OPEN SOURCE

Como optimizar Ubuntu en 7 pequeños pasos

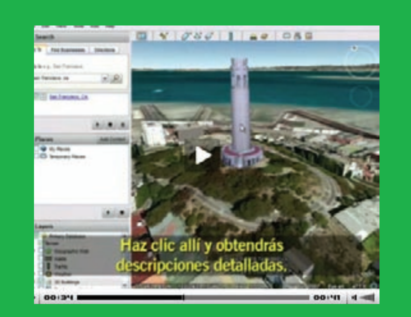
Generalmente, luego de una instalación fresca de Ubuntu, nos encontramos en maquinas mas antiguas una baja en el rendimiento general del sistema. En comparación con Debian Etch, el rendimiento se reduce un poco.



VIDEOS

Google Earth 4.3

Google lanzó la versión 4.3 del espectacular Google Earth, el cual incluye nuevas funcionalidades y herramientas que le permitirán recorrer cada lugar del planeta. Descúbralo.





www.sxc.hu - Sophie

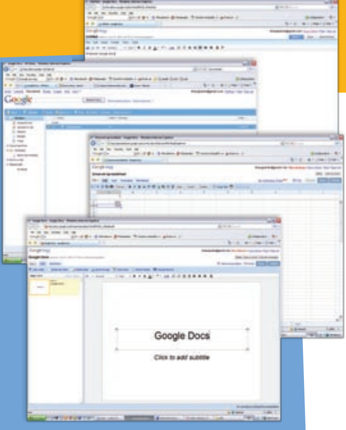
Suites de oficina online

La suite Microsoft Office no solo es la aplicación de oficina más exitosa y popular del mundo, sino que hasta hace poco tiempo era la única. Su combinación de procesador de texto con hojas de cálculo y software de presentación, entre otras funcionalidades, la hicieron imbatible. Otras aplicaciones como Lotus 1-2-3, WordPerfect o Harvard Graphics son testigos directos de esa popularidad. En otros tiempos fueron de los sistemas más populares para luego ser eclipsados totalmente por el Office.

Sin dudas, Microsoft ha recibido muchas críticas por las estrategias utilizadas para conseguir esta espectacular posición de privilegio, sin embargo los resultados no se ponen en discusión. Microsoft Office es la suite de oficina número uno.

No obstante, desde hace un tiempo no es la única. Una nueva generación de suites de oficina online se ha hecho presente. Gracias, en parte, al notable crecimiento de Internet y la explosión del acceso a altas velocidades, una nueva generación de aplicaciones online está empezando a competir con los tradicionales Word, Excel y PowerPoint. Los días de Microsoft como único jugador del mercado de aplicaciones de oficina evidentemente han terminado.

Una de las mayores ventajas que las nuevas suites ofrecen es que no necesitan almacenarse en nuestros equipos sino que las aplicaciones y los archivos se encuentran disponibles en la Web. Por ejemplo, Google Docs permite crear, editar, imprimir y guardar la hoja de cálculo, procesador de textos y la presentación de documentos sin necesidad de instalar una aplicación en la PC.
La otra ventaja es su costo, la mayoría de las aplicaciones se ofrecen gratis o a un precio mínimo, a diferencia de los costosos productos de Microsoft, y esta es una de las razones por la cual las aplicaciones online están siendo cada vez más utilizadas por los departamentos de IT.
La gran pregunta es si efectivamente alguna de estas nuevas suites tiene verdaderas oportunidades de competir con el producto de Microsoft. Para eso analizamos tres de las más populares suites de oficina online y les contamos cuáles son los resultados.



Google Docs

Si bien se trata de la suite online más conocida de todas, no ofrece todas las aplicaciones a las que el Office nos tiene acostumbrados. El Google Docs tradicional es muy recomendable para el hogar y la pequeña oficina, mientras que existe también una versión Premier con más aplicaciones, que incluye extras de seguridad y funciones de apoyo técnico para el uso de la empresa.

Por ejemplo, el Premier Edition incluye APIs que permiten a Google Docs integrarse fácilmente con la infraestructura existente de IT, ofrece 25 GB de espacio de almacenamiento, contra los 2,75 GB de la versión gratuita y proporciona acceso a la seguridad Postini entre otras funcionalidades orientadas a la empresa.

En cuanto al procesador de texto, Google ha hecho un gran trabajo preservando casi la misma apariencia y funcionalidades del Word. El Presentation es un software para presentaciones bastante similar al PowerPoint aunque con algunas ventajas en cuanto a que permite utilizarlo de manera colaborativa y el Google Spreadsheets por su parte es el equivalente al Excel.

En general, Google Docs resulta una interesante opción mientras que el reciente lanzamiento del Google Gears, que permite trabajar offline, para que una vez vuelto a conectar, los trabajos se sincronicen automáticamente, la hace aún más competitiva. Aunque tiene un conjunto limitado de características como para poder reemplazar definitivamente al Office, en especial en lo que hace a las necesidades de las empresas, no hay dudas de que la gente de Google está realizando un muy buen trabajo.

PROS: Estrecha integración con Gmail, probablemente el mejor servicio de correo electrónico, interesante espacio de almacenamiento para documentos, gran rendimiento y confiabilidad, excelente funcionalidad para compartir documentos. La nueva capacidad de trabajar también offline.

CONTRAS: No ofrece todas las características del Office, cosa que sí hacen otras suites online.

PRECIO: Gratis para edición estándar, mientras que la edición Premier tiene un costo de $50 dólares anuales por usuario.

RECOMENDACIÓN: Una buena alternativa de Microsoft Office para los usuarios domésticos y las pequeñas empresas que no necesitan todas las aplicaciones que ofrece el Office, sino más bien la posibilidad de compartir y revisar documentos en línea.

GOOGLE DOCS: WWW.GOOGLE.COM



Al igual que los otros productos de esta comparación, Zoho incluye sus propias versiones del Word, Excel y PowerPoint. El Zoho Writer es el procesador de texto, el Zoho Sheet una hoja de cálculo muy similar al Excel y el Zoho Show es un software de presentación parecido al PowerPoint. Sin embargo donde Zoho sobresale es en la profundidad y amplitud de los productos que ofrece, cerca de una docena de aplicaciones en línea para realizar las más diversas tareas, desde un gestor de clientes CRM hasta un software Wiki.

Zoho Meeting es una aplicación de conferencias Web, Zoho Projets administrador de proyectos, Zoho Creator permite la creación de mini-aplicaciones Web, Zoho Planner organizador personal y los mencionados Zoho Wiki y Zoho CRM son solo algunas de las aplicaciones que este paquete ofrece. En términos de compatibilidad Zoho Writer y Zoho Sheet no presentan problemas para cargar documentos de Word y Excel. El Zoho Show sin embargo muestra algunos problemas visuales al cargar documentos de PowerPoint, principalmente en cuanto al tamaño de algunas fuentes. No obstante la mayoría de los módulos de Zoho presentan grandes posibilidades de exportación. Por ejemplo la hoja de cálculo puede exportar trabajos en XLS, hoja de cálculo de OpenOffice, Gnumeric, CSV, HTML, XHTML y PDF. Zoho también ofrece un interesante plug-in que permite a los usuarios editar y guardar documentos directamente en Zoho desde el Word y el Excel.



Al igual que Google Docs y ThinkFree, Zoho proporciona un sólido apoyo para el intercambio de documentos con otros usuarios en línea, pero el Zoho además ofrece permanentemente una gran cantidad de actualizaciones y mejoras. Lo que quizás le falte a Zoho sea la apariencia profesional orientada a la oficina que ofrece el ThinkFree, no obstante indudablemente gana puntos por la amplitud de aplicaciones que ofrece así como además el rápido ritmo de sus actualizaciones.

PROS: Incluye más de una docena de aplicaciones, robusta capacidad de importación y exportación, brinda la posibilidad de trabajar fuera de línea, a través de Google Gears, y frecuentes actualizaciones y mejoras. Es gratuito.

CONTRAS: Una pobre interfaz que parece centrada en los usuarios domésticos y no en las empresas u oficinas. Algunos problemas de rendimiento como por ejemplo los mostrados por Zoho Show para importar archivos de PowerPoint.

PRECIO: Gratuito.

RECOMENDACIÓN: Si lo que se busca es una suite online y gratuita que ofrezca todas las aplicaciones del Office, Zoho sin dudas es la respuesta, ya que ofrece muchas más aplicaciones que las otras suites aquí evaluadas. Sin embargo no se puede decir aún que esta suite sea capaz de reemplazar en todas sus potencialidades al tradicional Office.

ZOHO OFFICE SUITE: WWW.ZOHO.COM



Se trata de la suite online más parecida al Office de Microsoft, hasta se podría decir que se trata de una copia exacta, con la única diferencia de que el ThinkFree se ofrece en línea. Presenta el mismo aspecto en casi todos los detalles, las mismas opciones de los distintos menús e incluso los mismos iconos. La similitud es intencionada y, según sus creadores, se ha realizado para evitar al usuario el aprendizaje de la herramienta si ya está familiarizado con otros programas como Microsoft Office. ThinkFree apunta principalmente a ofrecer paquetes destinados a las empresas y los usuarios de la empresa, lo que lo hace la mejor opción para usuarios de negocios que buscan una alternativa online al Office. ThinkFree Write es un procesador de texto, muy similar al Word, el ThinkFree Calc es una hoja de cálculo similar en funciones y aspecto al Excel, mientras que el ThinkFree Show es un software de presentaciones al estilo PowerPoint.

Pero además, ThinkFree Server permite a las empresas ejecutar el software en su propio servidor Web, ThinkFree Desktop es un servicio que permite descargar e instalar en la computadora los documentos, incluso sin conexión a Internet. ThinkFree brinda, gracias a una API, grandes posibilidades de integración con otras aplicaciones, además de la capacidad de trabajar offline y sincronizar luego. Esta suite ofrece dos posibilidades de funcionamiento, una versión Quick, básica y rápida basada en AJAX y compatible con la mayor parte de los equipos y sistemas, y una versión Power que requiere Java y una buena conexión. Otros detalles importantes son el soporte técnico que ofrece y la posibilidad de cargar varios archivos desde una sola pantalla. Por otro lado, carece de la gran cantidad de funcionalidades que ofrece el Zoho, así como su frecuencia en las actualizaciones. También corre detrás de Google en lo que se refiere a la funcionalidad del correo electrónico y calendario. Si bien aún no puede competir con el Office en lo que hace a las necesidades de grandes empresas, el ThinkFree es la mejor de las alternativas online para los hogares, las oficinas y las pequeñas empresas y además es gratuito.

ThinkFree: www.member.thinkfree.com/

Pros: Muy similar al Microsoft Office en cuanto a funcionalidades y aspecto. Gran capacidad para importar y exportar documentos de otros formatos, otorga la posibilidad de trabajar offline. Es gratuito.

Contras: Se desempeña de manera lenta con algunos documentos de gran tamaño si se lo compara con sus competidores. Las actualizaciones también son un poco lentas, sobre todo en comparación con Zoho. Carece de algunas aplicaciones.



Precio: Gratis para ThinkFree Premium, $30 por usuario y por año para ThinkFree Server Edition.

Recomendación: Si bien todavía no puede reemplazar al Office en la mayoría de los entornos de oficina, ThinkFree es la suite más competitiva de las que se ofrecen en línea en la actualidad y si se tiene en cuenta que se puede descargar gratis o pagando una pequeña suma en el caso del Server Edition, resulta una excelente opción.

¿La respuesta de Microsoft?

Que Microsoft haya tardado en responder a la avalancha de competidores de oficina basados en la Web, no debería sorprender. Una versión online del Office podría desmoronar las ventas de sus lucrativos productos de oficina empaquetados, los cuales son una de las mayores fuentes de ingresos de la compañía. Pero por otro lado, no podía quedarse de brazos cruzados viendo cómo sus nuevos competidores le quitaban cuota de mercado.

Por eso el 4 de marzo de 2008 Microsoft puso a disposición del público la beta de Microsoft Office Live Workspace, la cual no permite editar documentos online, sino manejarlos, compartirlos y tenerlos permanentemente disponibles de forma online.

Lo que busca básicamente la nueva aplicación es maximizar las posibilidades que otorga trabajar tanto online como offline.

Para poder utilizar el Office Live es necesario tener instalada una versión del Office para poder editar y guardar los documentos.

A pesar de que no ofrece la posibilidad de trabajar online, esta herramienta tiene algunas interesantes características si se la utiliza como un complemento del Office tradicional. La capacidad de almacenar documentos comunes para su posterior edición en cualquier lugar y a través de cualquier computadora es la principal, así como también la chance de compartir documentos de manera colaborativa.

Es que al carecer de una facultad que poseen las demás suites gratuitas antes evaluadas, es decir la posibilidad de editar y crear online, no se la puede considerar una competencia o una respuesta directa a estas nuevas herramientas, sino simplemente un buen complemento para el Office.

Las predicciones para 2008

"Conoce al enemigo y conócete a ti mismo y, en cien batallas, no correrás jamás el más mínimo peligro. Cuando no conozcas al enemigo pero te conozcas a ti mismo, por cada victoria obtenida sufrirás una derrota. Pero si no conoces ni al enemigo ni a ti mismo, sucumbirás en cada batalla". Sun Tzu

Desde hace ya varios años los ataques cibernéticos han estado evolucionando a un ritmo tan acelerado que han pasado de ser una rareza a poner en riesgo la seguridad de empresas y gobiernos. La frecuencia, sofisticación, diversidad y severidad de estos ataques han logrado tal grado de madurez que el mundo desarrollado se encuentra cada vez más expuesto. Además, las acciones de prevenciones y de defensa evolucionaron más lentamente que las amenazas, las cuales están soportadas por un mercado negro global y por gobiernos ambiciosos por programas de espionaje. Esto significa que la realidad será cada vez peor en vez de mejorar.



Conciente de esta situación, hace un tiempo ya que **VeriSign** lanza, junto a su grupo de iDefense Intelligence, el iDefense Security Report el cual analiza la situación actual y predice qué es lo que nos traerá este 2008.

Antes de abocarnos de lleno en la discusión sobre los peligros de 2008, vale recalcar que de las 27 predicciones para 2007, 23 de ellas fueron verificadas, 3 incorrectas y 1 dudosa, lo que le brindó un 85 por ciento de efectividad al estudio para el año pasado. De estas predicciones de iDefense para 2007, muchas de ellas eran bastante obvias, como que los ataques de spam aumentarían y que el phishing continuaría creciendo. Sin embargo, también se acertó acerca de desarrollos no tan evidentes, como el aumento de la especialización y diferenciación del mercado clandestino criminal, la emergencia de un cyber mercado clandestino en Europa del Este con una gran diversidad de operaciones y parecido a uno legítimo.

La preponderancia de la evidencia de 2007 sugiere que el mercado tecnológico clandestino está evolucionando y expandiéndose a grandes escalas. Por cerca de dos décadas, los hackers han operado de forma independiente o en pequeños grupos informales. Este tipo de organizaciones se mantienen, pero fueron dejados de lado por la aparición de dos nuevas formas: el cyber cartel y la cyber celda paramilitar.

El cyber cartel es una organización criminal y semi-informal que piensa y opera como una empresa, mientras que la celda paramilitar opera como una unidad militar irregular que está al servicio de un estado, un grupo social o una ideología.

Según el estudio, el liderazgo de los cyber carteles se consolidará y su negocio evolucionará, mientras que el mercado global continuará creciendo en alcance y diferenciación de funciones. Adoptarán más y más prácticas de negocios que ya fueron probadas por los líderes para lograr el éxito, y mejorarán sus productos, el proceso de desarrollo y el marketing. Invertirán en investigación, terciarizarán algunas de sus funciones y realizarán alianzas estratégicas tanto con economías legales como con ilegales. Tal es el grado de especialización y profesionalismo que alcanzarán los cyber carteles que casi no podrán ser distinguidos de las firmas legales, excepto por la característica de que el cartel tiene los riesgos y los costos de estar operando fuera de la ley y evadiendo el costo de trabajar legalmente, como por ejemplo el pago de impuestos.

El estudio de iDefense tiene tres ramas de análisis: **quiénes son los actores, cuáles son sus motivaciones y cuáles son sus métodos y tácticas.**

En cuanto a los **actores**, el reporte para 2008 hace foco en tres tipos de amenazas: los insiders, los hackers contratados y los atacantes regionales. A primera vista, la discusión sobre los actores regionales puede parecer fuera de lugar, pero la realidad muestra que la compleja intersección de factores políticos, económicos y sociales en cada parte del mundo influyen fuertemente sobre qué actividad del hacking predominará en cada región. Más concretamente los actores de una cierta región, por ejemplo Europa del Este, son más propensos



www.sxc.hu - Simon Cataudo



a las actividades relacionadas con el fraude cibernético, mientras que los hackers de China tienden más al cyber espionaje o al hackeo político.

En cuanto a porqué ciertos actores hacen lo que hacen surgen varios temas interesantes para discutir. En su momento, la prensa rápidamente etiquetó el ataque de denial of service de junio de 2007 contra Estonia como la primera guerra cibernética. Muchos Gobiernos de países del Este por primera vez y en forma conjunta hicieron pública su preocupación por las actividades de cyber espionaje llevadas adelante en China. Por su parte, los cyber terroristas islamitas demostraron que aún no están aptos, pero tienen claros signos de mejora y están en la búsqueda de apoyo mundial.
Otros cyber activistas con motivaciones que van desde lo político al medio ambiente aumentaron la cantidad y la severidad de las protestas en el cyber espacio. Finalmente, la historia más grande de 2007 fue la maduración del mundo criminal clandestino hacia una sub cultura, robusta y enteramente global apoyada por cientos de billones de dólares robados por individuos y por grupos organizados. El resultado es que, aunque la fuerza de la ley pueda desmantelar el mejor 10 por ciento de estos grupos, el mercado continuará siendo atractivo para nuevos participantes.

iDefense 2007 Predictions Scorecard

Correct	Unclear	Failed
Prediction Verified	Unclear	Prediction Incorrect
23	1	3
85%	4%	11%

La diversidad de la motivación detrás de los ataques aumentará durante 2008. Esto se refleja, en parte, en el crecimiento de los conocimientos técnicos de hackeo que posee la población mundial, pero también por la búsqueda de logros particulares. El motivo financiero es en la actualidad el dominante, y lo será aún más durante 2008, aunque los motivos políticos y estratégicos se volverán más visibles.

Con respecto a **los métodos y las tácticas**, se hace foco en varios ataques rastreados por VeriSign iDefense durante 2007. "Mientras que no emerjan nuevos tipos de ataques, los actores maliciosos realizan mejoras e innovaciones a sus herramientas y prácticas, muchas de las cuales serán al menos tan exitosas en 2008 como en años pasados".

Según explica el iDefense Security Report 2008, las herramientas de los hackers serán más refinadas y entre los desarrollos podemos esperar los siguientes:

- A los hackers les costará comprometer el nuevo sistema operativo Windows Vista aún cuando su venta continúe en descenso durant 2008.
- Los activistas o "hacktivistas" continuarán utilizando la Web como vehículo de protesta a través del uso coordinado de ataques de DoS.
- Se detendrá el aumento de los servidores Fast-Flux por sus altos costos y la baja demanda.
- La disminución de servidores IRC-based C&C comenzará en 2008 mientras son reemplazados por Web -y P2P- bootnets.

La seguridad de la información ya no es más un problema "técnico"; es un problema de todos y ya cada vez más gente da cuenta de esta situación. No solo las amenazas son más numerosas, serias y sofisticadas, sino que tanto líderes con gran conocimiento como el público en general están empezando a mostrar un nivel de preocupación proporcional a la realidad. Este aumento de preocupación es bienvenido pero llega un poco tarde. ¿Por qué? Las amenazas han crecido hasta llegar a un punto crítico en el cual son capaces de causar un daño inmenso a empresas, sectores económicos y a gobiernos.

Hasta el chequear la intensidad de este problema requeriría extrema atención, cientos de billones de dólares, cambios significativos de percepción y varios años de esfuerzo enfocados en proyectos que involucran la capacitación de diez mil profesionales alrededor del mundo. Todo esto demuestra que el desarrollo de soluciones para la amenaza cibernética no puede estar en control de una sola organización, ni en manos de una combinación de organizaciones, incluyendo gobiernos y multinacionales. Sin una solución a la vista, la defensa y la precaución se vuelven fundamentales para la supervivencia.

Aquellos que lo hagan relativamente bien aún experimentarán riesgos y pérdidas, pero aquellas empresa que tengan políticas más pobres no se mantendrán activas por mucho tiempo. Esto sugiere que la única solución confiable resta en individuos bien entrenados, organizados y con acceso a información de punta respecto a las amenazas contra las que tienen que pelear.

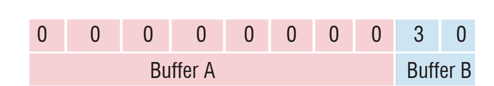
ATAQUES DE BUFFER-OVERFLOWS

Un buffer-overflow (también conocido como buffer-overrun) ocurre cuando una aplicación mal programada guarda datos en la memoria de la computadora, más allá de los límites de un buffer de longitud-fija.

Como resultado los datos extra, que desbordan (overflow), sobreescriben lugares de memoria adyacentes. Los datos que son reemplazados pueden incluir otros datos, variables o lógicas de programas y pueden hacer que un proceso haga un crash (se detenga) o produzca resultados incorrectos.
Una amenaza mayor sucede cuando los datos inyectados son código ejecutable que el programa bajo ataque es obligado a ejecutar. Este código ejecutable es normalmente el llamado "payload" real de este tipo de ataque.

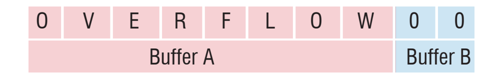
Para qué se utiliza este tipo de ataque: destruir o robar datos, perturbar servicios creando un Denial of Service (DoS - denegación de servicio), causar elevación de privilegios o desparramar malware a otros sistemas.

Veamos un ejemplo simple de un "buffer overrun".
Un programa tiene definidos dos variables que están almacenadas en lugares de memoria adyacentes: un buffer de 8 bytes tipo string, A, y otro de dos bytes tipo entero, B.
Inicialmente, X contiene nada más que ceros y B un número entero: 30.



0	0	0	0	0	0	0	0	3	0
Buffer A								Buffer B	

Supongamos que un usuario (en algún formulario o password) sin intención o maliciosamente, introduce el string OVERFLOW en el programa.



O	V	E	R	F	L	O	W	0	0
Buffer A								Buffer B	

El programa intenta poner el string "OVERFLOW" en el lugar de memoria reservado para A. También pondrá un cero al final indicando el final del string. Si la lógica del programa no checkea la longitud máxima asignada a A, se escribirá el 0 arriba del 3 de B.

Resultado: aún cuando el programador nunca planeó dejar a Y en cero al poner algo en X, ese es el resultado.

Los llamados "boundary checks" en las plataformas de programación actuales fueron desarrollados para evitar este tipo de problemas. Los "boundary checks" aseguran entonces que los datos que se entran sean de las longitudes apropiadas. Pero existe mucho código "legacy" (heredado, antiguo, anterior) aún en uso, donde esta práctica no se realizaba. Además aún actualmente muchos desarrolladores no siguen estas "best practices" y aún hoy aparecen los buffer overruns en código nuevo.

Estas razones explican porqué muchos vendors de hardware, aplicaciones y sistemas operativos han desarrollado defensas proactivas para poder detener los ataques de buffer overflow sobre código mal programado.

Historia

Los ataques basados en buffer overflows han estado vigentes desde 1988 cuando el primer ataque del gusano Morris Worm se realizó distribuido vía Internet. Lo curioso es que los autores del gusano lo hicieron para medir la extensión de Internet y no para causar daño. Se basaba en passwords débiles y conocidas vulnerabilidades de los programas unix "sendmail" y "finger".

Los ataques más recientes utilizando la técnica de buffer-overrun, los gusanos Code Red y SQL Slammer, expusieron al abuso de los hackers a muchas computadoras interconectadas a Internet. Code Red en 2001 lo hizo sobre una vulnerabilidad de Microsoft Internet Information Services (IIS) 5.0 (el web server que estaba por default en Windows 2000). En 2003 fueron los servidores de base de datos que corrían Microsoft SQL Server 2000 los que fueron comprometidos por SQL Slammer.

DEP (Data Execution prevention)

Uno puede prevenir la ejecución de código malicioso inyectado usando DEP. Éste permite que un sistema operativo (Windows o Linux, por ejemplo) marque lugares en memoria que deberían contener data NO-ejecutable (NX). Cuando una aplicación intente correr código de estos lugares de memoria marcados como NX, serán bloqueados.
Algo negativo respecto de DEP es que la aplicación bloqueada dejará de correr. Esto es aunque DEP logre que el código malicioso no pueda ejecutarse, se está creando una nueva oportunidad para que los hackers realicen un ataque de DOS (Denial of Service). Microsoft incluye soporte de DEP no solo en Vista y Windows Server 2008, sino también en XP SP2, Windows Server 2003 SP1 y R2. La implementación de DEP viene en dos variantes: Hardware-enforced DEP y Software–enforced DEP.

Hardware-enforced DEP: Tanto AMD como Intel proveen DEP en algunos de sus procesadores bajo los nombres Non-Execute Page Protection (NX) y Execute Disable Bit (XD) respectivamente. Microsoft no es el único vendor de Sistemas Operativos que utiliza

esta característica a nivel de hardware. Linux y BSD también lo proveen (ver en.wikipedia.org/wiki/Nx-bit).

Software-enforced DEP: Por software Microsoft por ejemplo provee DEP en procesadores de 32 bits no equipados con procesadores provistos de NX o XD. Referimos al lector al knowledge base de MS (support.microsoft.com/kb/875352/en-us) para obtener detalles de cómo verificar si DEP puede ser usado en hardware o cómo implementarlo como software.

ASLR
(Adress Space Layout Randomization)

ASLR es otra técnica comúnmente utilizada para defendernos de exploits basados en "buffer overruns".

¿Qué es entonces ASLR? Cuando uno bootea una computadora, cargamos código del sistema en diferentes lugares de la memoria. Existen muchos ataques, ya muy bien entendidos llamados "return to libc", donde un exploit intenta llamar una "system function", como por ejemplo socket() en wsock32.dll. De este modo abriría un socket o LoadLibrary en kernel32.dll y cargaría wsock32.dll en primer lugar. La función de ASLR es mover los entry points de estas funciones a diferentes lugares de la memoria de modo que estén en lugares no predecibles para el malware. En el caso de Windows Vista una DLL o EXE podría ser cargado en cualquiera de las 256 posiciones. Esto significa que el atacante ve reducidas las chances de obtener el direccionamiento correcto en 256 veces. En síntesis, hace más difícil que los exploits funcionen correctamente.

Por ejemplo, en un arranque del sistema operativo diferente DLLs podrían estar en lugares como:

- wsock32.dll (0x73ad0000)
- winhttp.dll (0x74020000)
- user32.dll (0x779b0000)
- kernel32.dll (0x77c10000)
- gdi32.dll (0x77a50000)

Si se rebootea, ASLR podría modificarlos a:

- wsock32.dll (0x73200000)
- winhttp.dll (0x73760000)
- user32.dll (0x770f0000)
- kernel32.dll (0x77350000)
- gdi32.dll (0x77190000)

Como se puede observar las varias DLLs son cargadas en diferentes direcciones lo que hace mucho menos probable que un exploit localice el DLL y tome ventaja de las funcionalidades que posee. O sea no evita 100 por ciento pero le hace la tarea al código malicioso mucho más compleja y menos probable su éxito.

Resumen

Por tanto DEP y ASLR no son una panacea para código inseguro que puede ser comprometido por "buffer overflows". Pero, usados en conjunto con otras tecnologías, servirán para incrementar la seguridad de nuestra infraestructura IT. ●

Microsoft Visual C++ Runtime Library



Buffer overrun detected!

BUFFER: En general se entiende como "buffer" a un almacenamiento temporario. Puede ser, por ejemplo, en la memoria de la computadora. Es un espacio de la memoria de la computadora, en el que se almacenan datos de modo que el recurso que los requiere, ya sea hardware o software, pueda acceder a ellos en cualquier momento.
También es posible que "buffer" sea usado para nombrar el área de nuestra computadora/dispositivo que almacena datos en forma temporaria para ser transferidos entre por ejemplo dos máquinas o dispositivos que procesan los datos a diferente velocidades. Ejemplo computadora-impresora.

OVERFLOW: Desbordamiento.

DENIAL OF SERVICE (DENEGACIÓN DE SERVICIO). En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

DLL: Es el acrónimo de Dynamic Linking Library (Bibliotecas de Enlace Dinámico), término con el que se refiere a los archivos con código ejecutable que se cargan bajo demanda del programa por parte del sistema operativo. Esta denominación se refiere a los sistemas operativos Windows siendo la extensión con la que se identifican los ficheros, aunque el concepto existe en prácticamente todos los sistemas operativos modernos.

Fuente: wikipedia.org

6 modos absurdos de asegurar una RED LAN inalámbrica

Hace ya más de dos años, George Ou (http://blogs.zdnet.com/Ou/) escribió un artículo sobre modos absurdos (seis en total) de intentar lograr una red wireless segura. Este fue, quizás, su blog más exitoso, con dos flashes en Digg. Hoy tiene un ebook gratuito y muy bueno que puede bajarse de www.techrepublic.com. En este artículo revisaremos las 6 categorías propuestas por Ou.

www.sxc.hu - Dominik Rusiecki

Ou llama a estas metodologías "leyendas urbanas" en seguridad wireless y ha intentado por diversos medios de desterrarlas. Muchos las consideran "mejores prácticas" y son recomendadas incluso por algunas certificaciones internacionales muy prestigiosas como CISSP (ww.isc2.org), VISA (en su requerimientos y recomendaciones) y PCI (Payment Card Industry) Security Standards (www.pcisecuritystandards.org).

Los 6 modos absurdos
(fuente blog de George Ou)

01. MAC filtering

Esto es como darle a un guardia de seguridad un bloc de notas con una lista. Cuando alguien llega a la puerta y quiere entrar, el guardia de seguridad mira el nombre en la credencial que trae colgada y lo compara con su lista. Así determina si abre la puerta o no. Todo lo que se necesita hacer para vulnerar la seguridad es ver a alguien entrar y copiar su nombre en una credencial. El nombre en la credencial es en una red inalámbrica el MAC address (número HEXAdecimal único asociado a la placa de red) que puede ser detectado en modo texto por cualquier sniffer. Un sniffer es a un hacker como un martillo a un carpintero, con la diferencia de que el sniffer es gratis. Una vez que logra ver el MAC address en texto plano, le tomará 10 segundos hacer cut-paste y legitimarlo en el seteo de su placa de red wireless.

MAC filtering es de absolutamente ningún valor ya que representa uno de los esquemas más sencillos de vulnerar. Lo interesante es que aún en muchas organizaciones pierden tiempo en su implementación. Resumen MAC filtering lleva tiempo de implementación con CERO ROI (Return On Investment) en términos de mejora en la seguridad.

02. Escondiendo el SSID

No existe manera de hacer "SSID hiding" (esconder el SSID). Solo podremos esconder la divulgación a través del beaconing en el Access Point. Hay otros cuatro mecanismos que también hacen broadcast del SSID en el espectro de 2.4 ó 5.0 GHz. Los cuatro mecanismos son: probe request, probe responses, requests de asociación y requests de re-asociación. Esencialmente escondemos uno de los cinco mecanismos en que se hace broadcast del SSID. Nada hemos escondido y causaremos problemas al roaming del cliente cuando éste salte de un access point a otro. Esconder el SSID hace que nuestra red inalámbrica sea menos user-friendly. Si desea conocer más lea el white paper de Robert Moskowitz (Senior Director del ICSA Lab): "Destronando el mito de esconder el SSID".

03. Autenticación LEAP

La utilización de la autenticación LEAP de Cisco continúa siendo el error más grave que cometen las empresas a sus LANs inalámbricas ya que se quedan expuestas a ataques. Cisco sigue diciendo que LEAP es útil si se utilizan passwords largos.

El problema es que los passwords largos es algo que los humanos se niegan a utilizar. Si duda esto, haga una auditoria sobre los passwords en su empresa y vea cuánto tarda en crackear el 99 por ciento de ellos. Cualquier intento de forzar esta política llevará a la aparición de stickers en las computadoras con los passwords escritos en ellos.

Desde que Joshua Wright expuso una herramienta capaz de crackear LEAP con velocidad casi instantánea, Cisco se vio forzado a sacar una alternativa: EAP-FAST. Desafortunadamente EAP-FAST es aún inseguro en su instalación por default. Aunque Cisco provee gratis LEAP y EAP-FAST para las máquinas clientes, no es así para los access points. LEAP y EAP-FAST son dos protocolos propietarios de Cisco. Existen mecanismos basados en estándares abiertos como EAP-TLS, EAP-TTLS y PEAP que son más seguros que LEAP y EAP-FAST y funcionan en todos los access points y clientes, no solo Cisco.

Cisco no soporta estándares abiertos EAP como el resto, así que es muy recomendable utilizar siempre un EAP de estándar abierto y evitar el hardware lock-out.

04. Desabilitar DHCP

Esto es más una pérdida de tiempo que una mejora en la seguridad. DHCP permite la asignación automática de números IP y otras configuraciones.
Deshabilitar DHCP significa cero en mejorar la seguridad y se pierde tiempo. Le llevará solo 10 segundos a un hacker conocer los números IP asignados de una red y simplemente reasignarlos a su conveniencia.

Servidor/sonda/infraestructura cliente

Kismet tiene tres partes diferenciadas. Una Sonda que puede usarse para recoger paquetes, que son enviados a un servidor para su interpretación. Un *servidor* que puede o bien ser usado en conjunción con una sonda, o consigo mismo, interpretando los datos de los paquetes, extrapolando la información inalámbrica, y organizándola. El *cliente* se comunica con el servidor y muestra la información que el servidor recoge.

*Fuente Wikipedia

05. Posicionamiento de las antenas

Han habido muchos consejos sin sentido de expertos de seguridad informática, como solo colocar las antenas de los access point en cen-

Kismet

(Ver NEX #30, página 18)

Kismet es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas 802.11. Funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a y 802.11g. El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. El cliente puede también funcionar en Windows, aunque la única fuente entrante de paquetes compatible es otra sonda.

Características

Kismet se diferencia de la mayoría de los otros sniffers inalámbricos en su funcionamiento pasivo. Es decir que lo hace sin enviar ningún paquete detectable, permitiendo detectar la presencia de varios puntos de acceso y clientes inalámbricos, asociando unos con otros.
Kismet también incluye características básicas de Sistemas de detección de intrusos como detectar programas de rastreo inalámbricos incluyendo a NetStumbler, así como también ciertos ataques de red inalámbricos.

tro de los edificios y poner la potencia al mínimo. Recordemos que el hacker tendrá siempre una antena mejor y podrá detectar señal desde a más de 1.500 metros. Hacer la señal más débil es hacer funcionar la red inalámbrica mal. El posicionamiento de la antena y potencia de la señal deberá siempre ser la de máxima cobertura y mínima interferencia. Nunca deberá ser usada como medida de seguridad.

06. Solo use 802.11a o Bluetooth

Por suerte esta ya se escucha muy poco.
WEP un caso especial: Alguno de Uds. se preguntarán porque no aparece el uso de WEP como uno de los 6 modos absurdos en seguridad wireless. Desde hace ya un tiempo, toma solo unos minutos romper la seguridad WEP y por tanto podría ser candidata a la lista. Aún no fue incluida ya que por lo menos deja afuera de nuestra red a los hackers por unos minutos, requiere de ciertos conocimientos para largar los ataques de inyección de paquetes y no se ha propagado como una "leyenda urbana". Esto NO significa que se deba usar WEP.

Repercusiones

Es muy interesante conocer los comentarios que escucha Ou sobre el tema:

- ¿Cuál es el daño? Es una metodología por capas a la seguridad.
- Nos hace más difíciles de ser visualizados y hackeados.
- Somos una empresa pequeña y no tenemos recursos para seguridad más efectiva.

Ou responde a éstos argumentando en que se basan en presunciones equivocadas y un conocimiento errado de cómo funciona la seguridad wireless.
Su respuesta:

- Estas no son metodologías por capas. Es más como comprar seguros de garantía superpuestos ya que el beneficio real a hackers robando bandwidth ya está cubierto por medidas de seguridad reales. El daño está en que la gente confunde estos métodos con algo real y gastan más dinero y esfuerzo implementado algo equivocado y terminan por obviar medidas efectuadas.
- Implementarlas no nos hace más difíciles de ser hackeados. Kismet (ver recuadro) al escanear las ondas transmitidas revelará los llamados SSIDs escondidos, direcciones MAC y esquemas estáticos de números IP en cuestión de segundos.
- Si nuestro presupuesto es reducido usemos medidas efectivas.

Ou resume la implementación de seguridad wireless fuerte y efectiva en redes inalámbricas para el hogar y la pequeña oficina (SOHO) en un párrafo: **use seguridad WPA-PSK con una passphrase random (al azar) con un mínimo de 10 caracteres**. Hackear un password como ésta llevaría a un experto a usar alrededor de 10.000 computadoras single-core modernas en paralelo trabajando alrededor de 500 años. Si su hardware no soporta WPA, muy probablemente pueda obtener un upgrade de software/firmware gratuito para soportarlo. ●

SSID

El **SSID** (**S**ervice **S**et **ID**entifier) es un código incluido en todos los paquetes de una red inalámbrica WiFi para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.
Existen algunas variantes principales del SSID. Las redes *ad-hoc*, que consisten en máquinas cliente sin un Access point utilizan el BSSID (*Basic Service Set Identifier*); mientras que en las *redes en modo infraestructura* (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red y se divulga haciendo broadcast desde el Access point.

* Fuente Wikipedia, corregida

Cómo crackear una red LAN wireless





Muy probablemente su red wireless empresarial es vulnerable a una autenticación ineficaz que no solo expone su red interna sino todos los accesos de control de sus servidores.

Hace pocos días los investigadores en seguridad Joshua Wright y Brad Antoniewickz divulgaron una herramienta de penetración llamada FreeRADIUS-WPE que se basa en las debilidades de los clientes wireless de diferentes Sistemas Operativos (SO).

Lo primero que uno se pregunta es porqué divulgan tal herramienta, ya que tanto los "buenos" como los "malos" tendrán acceso a ella. La respuesta en seguridad informática es "awareness" (concientización).

Si no se hiciese así, muy probablemente nadie tomaría conciencia de los posibles daños hasta que suceden. Sin la exposición de la herramienta el problema de todos modos existe y será explotado tarde o temprano por algún "malo". Muy seguramente ahora que la herramienta está disponible, muchos auditores de seguridad la usarán para detectar esta vulnerabilidad en redes inalámbricas.

El problema

El diseño de los clientes wireless de la mayoría de los sistemas operativos (Microsoft, Apple o Funk) es aún muy pobre. Uno puede utilizar los protocolos de autenticación más potentes (PEAP, EAP-FAST o EAP-TTLS) y los algoritmos de encriptación más modernos como AES y aún ser blanco fácil. Los clientes wireless de hoy no permiten darnos cuenta si estamos siendo engañados o no.

Más técnico

En la autenticación en una LAN wireless con autenticación EAP no existe una manera natural o intuitiva de matchear el nombre en el certificado digital al nombre SSID. Más específicamente, el campo "subject" (también conocido como CN "Common Name" o DN , "Designated Name"), en el certificado digital del servidor que autentica puede ser denotado con cualquier nombre que querramos.

La mayoría de las organizaciones tendrán como mínimo alguna parte del nombre de la empresa en el certificado y si el certificado fue comprado a una Autoridad Certificante, el nombre del dominio estará al final del campo subject.

¿Pasa lo mismo con autenticación vía Web browsers?

La respuesta es NO.



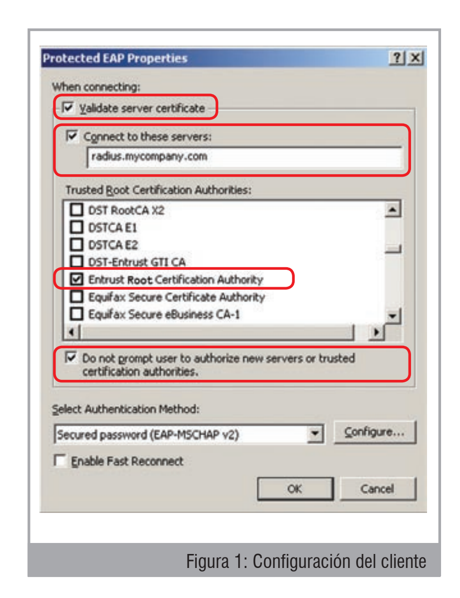


Figura 1: Configuración del cliente

Los clientes autenticados vía HTTPS (Hyper Text Transmition Protocol Security) mediante un Web Browser (Internet Explorer, Firefox) automáticamente validan el dominio en la dirección URL al campo subject del certificado.

Por lo tanto si accedo al sitio https://www.mibanco.com.ar, utilizando SSL/TLS y si el subject en el certificado en el servidor contiene el dominio mibanco.com.ar, se prende/activa un candado y se asegura que una entidad como por ejemplo VeriSign o Entrust nos verifican que estamos en un servidor del dominio mibanco.com.ar.

Pero para un cliente wireless que utiliza una autenticación basada en TLS usando EAP la cosa no es tan simple. Si uno detecta una red inalámbrica con SSID "miempresa", el certificado puede contener un nombre corporativo que nada tiene que ver con el SSID.

Cómo protegernos con productos Microsoft

George Ou es Technical Director de ZDNet y en un artículo reciente propone las siguientes medidas para los clientes de Windows XP, SP2 o Vista.

Cuando un cliente wireless XP, SP2 o Vista es instalado utilizando Group Policy, éste ofrece el mayor nivel de lockdown posible, siempre y cuando el administrador sepa hacerlo.

La configuración de un cliente wireless stand-alone, por otro lado no es solo confusa, sino que es errada ya que esconde la posibilidad de no visualizar el nombre del certificado. Cuando un usuario recibe un nuevo certificado solo ve el símbolo VeriSign pero el nombre en el certificado está escondido y puede por tanto ser engañado al hacer la conexión.

Sin embargo uno puede en XP, SP2 y Vista hacer un lock-down de modo que el usuario nunca sea requerido por un servidor RADIUS engañoso. Pero debemos setear correctamente la máquina cliente.

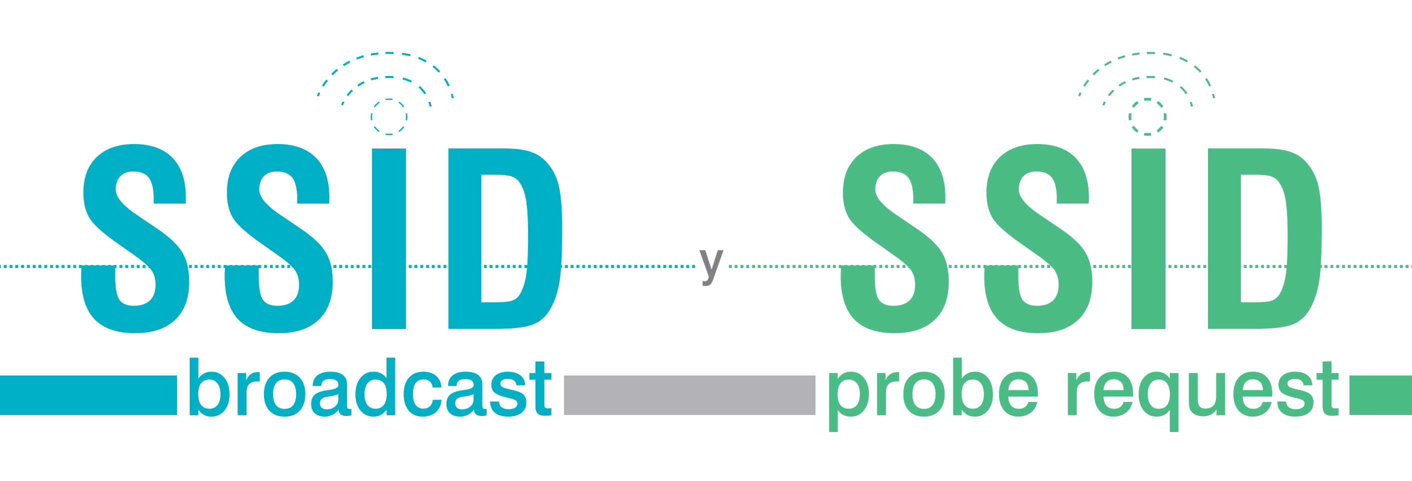
La figura 1 (Ou tiene además un excelente e-book gratuito en www.techrepublic.com que nuestro lector puede bajarse) nos enseña cómo hay que configurar al cliente. •



Lo importante es

- Tildar "validate server certificate".
- El campo "Connect to these servers" en el cliente wireless especifica el campo subject en el certificado digital X.509 (CN o DN). Otros nombres de servidores adicionales se pueden agregar separado por punto y coma.
- La calidad de autoridad certificante (CA, Certificate Authority) debe ser puesta explícitamente: pública o privada.
- La opción "do-not-prompt user to authorize new servers or trusted certificate authorities" fue clave para realzar la seguridad del cliente wireless en Windows.

Si alguna de estos detalles le parece confuso, ¡¡¡No es Ud. el único!!!



SSID broadcast y SSID probe request

Hoy existen herramientas de penetración como KARMA y FreeRADIUS-WPE que hacen que usuarios comunes y empresas se hallen más vulnerables que nunca cuando acceden a sus redes inalámbricas WiFi. Muchos creen (incluyendo recomendaciones dadas por algunas instituciones como PCI standard v1.1) que suprimir el SSID broadcast en el Access Point (AP) es la solución y resuelve el problema. La realidad es mucho más compleja.

Para aquellos expertos en wireless o seguridad, los primeros párrafos de este artículo les resultarán solo un repaso y el interés será generado solo al final del artículo.

La primera parte, entonces, está dirigida a aquellos que conocen poco de redes inalámbricas y su seguridad operando bajo WiFi (protocolo 802.11).

Conceptos básicos de redes inalámbricas

ABC del protocolo 802.11

El protocolo IEEE 802.11 es un estándar de protocolo de comunicaciones del Instituto de Ingenieros Eléctricos y Electrónicos, que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN(gíreles Local Area Network). En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz.

En la actualidad la mayoría de los productos son de la especificación b y de la g. El siguiente paso se dará con la norma 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen un primer borrador del estándar N con un máximo de 300 Mbps (80-100 estables).

El protocolo o estándar es el encargado de poner las normas y condiciones o definir los parámetros para que un elemento inalámbrico pueda acceder al medio y transmitir o recibir información.

El protocolo 802.11 usa el aire como medio de transmisión a una frecuencia no regulada, de libre emisión.
El estándar además se encarga de definir la forma en que accederemos a este medio, es decir, se marcan una serie de acciones que debe ejecutar el emisor antes de poder enviar ningún mensaje de forma que cuando transmita no pueda hacerlo ningún otro nodo.

Wi-Fi

Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11. Wi-Fi no tiene ningún significado ni es acrónimo de nada. Es sólo una marca, un sello que sirve para certificar que un producto cumple con los estándares 802.11.

RADIUS

Acrónimo en inglés de **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**erver. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones. Fue originalmente desarrollado por Livingston Enterprises y publicado en 1997 como los RFC 2058 y 2059.

Actualmente existen muchos servidores RA-

DIUS, tanto comerciales como de código abierto.

FreeRADIUS

Es un demonio de autentificación en Internet que deriva del protocolo Radius, aunque éste, como su nombre lo indica, es libre. Es utilizado para administrar el acceso remoto y la movilidad IP, como ocurre en servicios de acceso por modem, DSL, servicios inalámbricos 802.11 o servicios de VoIP (Voz sobre IP). Usar FreeRADIUS permite autentificación y autorización para una red centralizada y minimiza el trabajo de reconfiguración que se debe hacer al añadir o eliminar usuarios. Cuando se utiliza en conjunción con la AP puede dar acceso no autorizado a la red inalámbrica.

Modos Ad-hoc e infrestructura

Las redes inalámbricas se configuran en uno de 2 modos: Ad-Hoc o Infraestructura.

Qué es **modo infraestructura**: Es una manera de implementar nuestra red inalámbrica WiFi (802.11), en donde cada dispositivo (computadora) se comunica con los otros siempre a través de un Acess Point (AP).
En modo infraestructura los nodos inalámbricos se comunican entre sí o pueden acceder a otros dispositivos conectados por cable. Estos pueden ser por ejemplo computadoras que den servicios de fileservers o impresoras. El AP también puede routear a Internet (ver figura 1).

Qué es **modo Ad-hoc:** Ad hoc es una expresión que significa "para esto". Hace referencia a una solución elaborada específicamente para un problema o un fin preciso y, por esto, no es generalizable ni utilizable para otros propósitos. Se utiliza para referirse a algo que es adecuado sólo para un determinado fin. En sentido amplio, ad hoc puede traducirse como "específico" o "específicamente".
En el mundo de redes wireless indica que NO existe en nuestra configuración un nodo central administrador, sino que todos los nodos (computadoras) están en igualdad de jerarquía y función (ver figura 2).

Qué es el **SSID**: Es el anacronismo para Service Set IDentifier, un identificador único de 32 caracteres asociado al "header" de los "paquetes" enviados en una red inalámbrica (WLAN, Wireless Local Area Network) y que actúa como un password cuando un dispositivo inalámbrico trata de conectarse a la red. En el caso de modo infraestructura a través AP, el SSID diferencia una WLAN de otra, por tanto

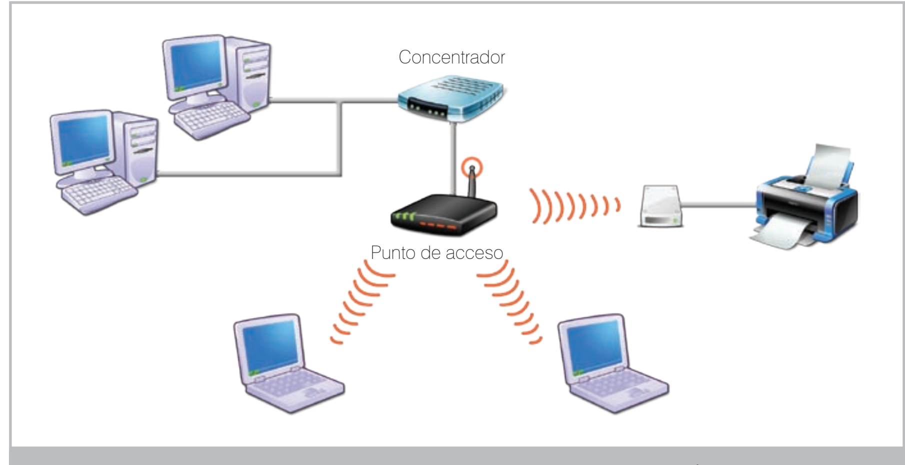


Figura 1: Modo Infraestructura



Sitio web de Joshua Wright: http://www.willhackforsushi.com

el AP y todos los dispositivos que intentan asociarse deberán poseer el mismo SSID.
Un dispositivo NO podrá ser parte de la red a menos que pueda proveer el SSID único. El SSID es fácil de ser detectado por los sniffers en texto plano y provee poca seguridad a la red. El SSID es referido muchas veces como "nombre de red" (network name).

SSID broadcast y SSID probe request

Existen cinco mecanismos paralelos de divulgación del SSID: SSID beaconing (al igual que como se sucede en el lenguaje de la navegación, beaconing es una señal constante que tiene la función de señalar un camino o punto de acceso, como la luz de los faros o las balizas de los aeropuertos) en el AP, probe request, probe responses, requests de asociación y requests de re-asociación.

¿Se puede entonces suprimir el beacon en el AP y así esconder el SSID? La respuesta es NO. Ya que como comentamos antes hay otros cuatro mecanismos donde se hace el broadcast SSID.

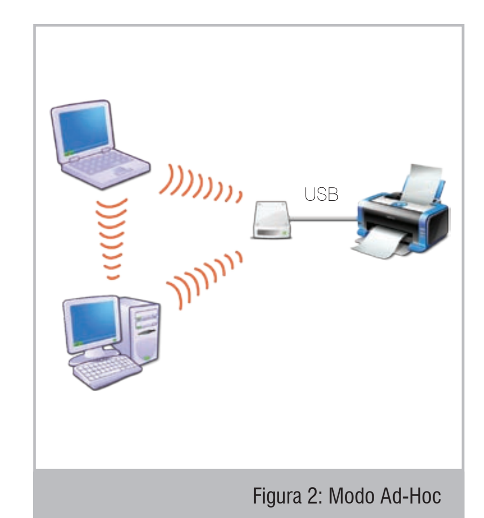


Figura 2: Modo Ad-Hoc

Por tanto no es solo inútil suprimir el beaconing del SSID en nuestro AP, sino que así obligamos a los clientes a revelar en forma constante su presencia y hacer broadcast del SSID de la empresa a todo lugar que vayan. Por modificar el AP nuestros (muchos) clientes (usuarios que desean conectarse) hacen broadcast de SSID en los llamados "probe requests" haciéndolos muy vulnerables. Una herramien-

HERRAMIENTAS DE PENETRACIÓN

KARMA

Es un conjunto de herramientas para testear la seguridad de los clientes inalámbricos en múltiples capas. Lo hace a través de la explotación de ciertos problemas en la forma en que trabaja 802.11 y además crea todo un framework que permite explotar en diversas formas a los usuarios conectados. Esta nueva herramienta para explotar las vulnerabilidades de las conexiones inalámbricas fue desarrollada en parte por Dino Dai Zovi, uno de los hackers más reconocidos del mundo, famoso por haber crackeado una Mac en un evento en Canadá este año.

FRERADIUS-WPE (Wireless Pwnage Edition)

Se trata de un parche para el demonio Open Source FreeRADIUS. Es una aplicación que sirve para demostrar las vulnerabilidades por suplantación, creado por Joshua Wright y Brad Antoniewicz. Es una herramienta muy valorada por los hackers ya que, dependiendo de cómo se la use, permite oír los "probe requests" de los clientes y hacerse pasar por el AP.

Entre otras cosas esta herramienta permite:

01. Simplificar la configuración de FreeRADIUS añadiendo todas las direcciones RFC1918 como dispositivos aceptables de NAS;

02. Simplificar la configuración de la autenticación EAP mediante la inclusión de soporte para todos los tipos de FreeRADIUS que soportan EAP;

03. Añadir WPE acceder prefijo $ / var / log / Radio / freeradius-servidor-wpe.log, lo que puede ser controlado en radius.conf cambiando el "wpelogfile" directiva.

04. Simplificar la configuración de la autenticación del usuario por defecto con un archivo "users" que acepte la autenticación de cualquier nombre de usuario.

Joshua Wright es un respetado investigador de seguridad, especializado en Wireless, y se desempeña como autor y profesor en el SANS Institute. Es además el responsable del sitio www.willhackforsushi.com, según él porque como nunca le interesó el dinero, su filosofía de trabajo muchas veces lo terminaba empujando a recibir como compensación uno o dos platos de sushi. Hackear por el sushi entonces resume su historia.

Brad Antoniewicz trabaja para Foundstone, una división de McAfee, que es una de las consultoras líderes en seguridad informática.

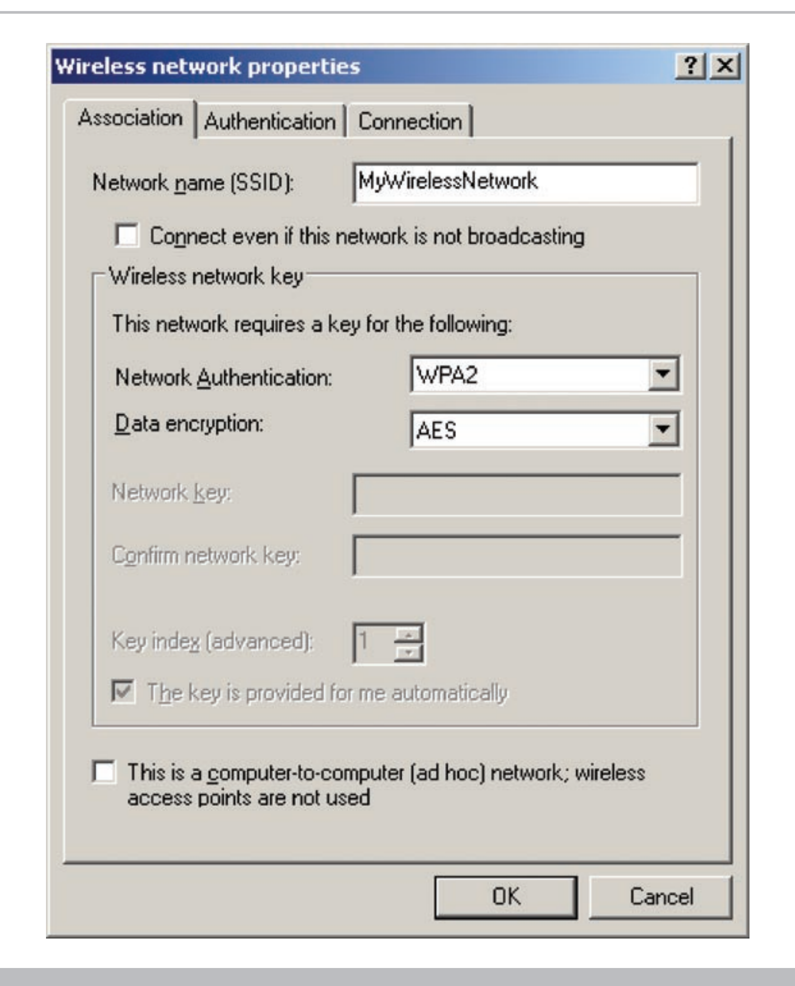


Figura 3: Cómo setear las propiedades de la red

ta como FreeRADIUS-WPE en manos de un hacker puede oír los "probe requests" de los clientes y hacerse pasar por el AP y cosechar lo necesario para un cracking fuera de línea. Si esto sucede no tardará en ser hackeada su red ya que las credenciales de los usuarios han sido comprometidas.

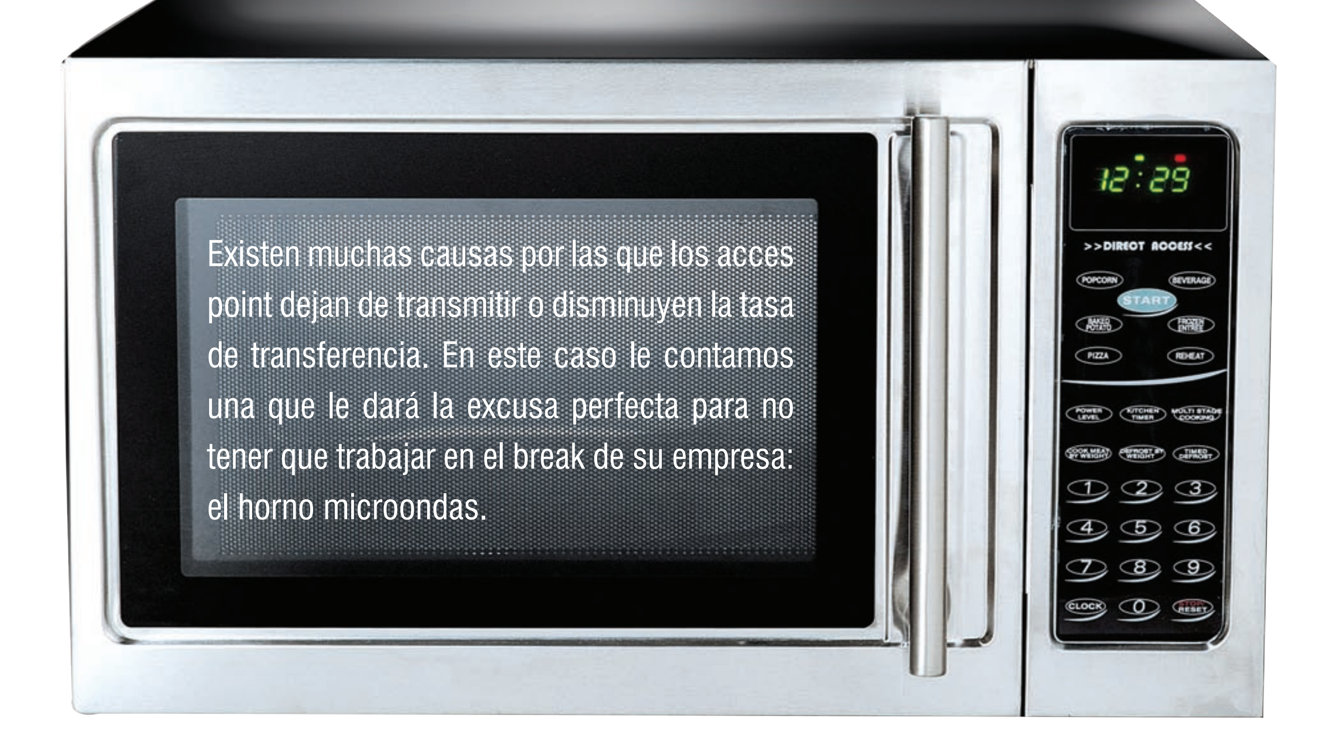
Entonces no nos conviene silenciar los "probe request". Si hacemos esto nadie sabe que alguien quiere conectarse. Alguien tiene que comenzar a pedir conexión. Si el AP o el cliente lo hacen, asumirán que no existe la posibilidad. Si el AP beaconea el SSID, el cliente podrá operar en el llamado modo "stealth" (silencioso) algo importante cuando están en la calle.

Caso de XP y Vista

Microsoft tiene para XP un "wireless client patch" que fue originalmente lanzado en 2004 y presentó importantes mejoras los años siguientes. Es un add-on a XP con Service Pack 2 y viene incluido en Windows Vista. Suprime por defecto el lado cliente de los probes de SSID. Sin embargo, se ve forzado a permitir SSID probes en el caso que el AP no broadcastee el SSID.

Como vemos en la figura 3, si en Windows XP o Vista se habilita "Connect even if this network is not broadcasting" que está off por defecto, nos transformamos en presa fácil de cualquier hacker que merodee nuestro entorno. •





Las interferencias en la radio frecuencia (RF) hacen que los clientes wireless y los access points dejen de transmitir, lo que provoca retrasos y una baja tasa de transferencia. En los casos en donde la interferencia de señales sea lo suficientemente fuerte, los clientes wireless puede que no logren acceder a la LAN durante un período indeterminado de tiempo. Es raro, pero posible.

Por tanto, es necesario estar conciente de las posibles causas de la interferencia en RF, como otras WLANs o los hornos microondas. Es por esto que en este artículo nos centraremos en la interferencia que genera un horno de este tipo. Muchas microondas emiten señales que cae con la propia banda de frecuencia de 2.4 GHz que la 802.11b WLANs utiliza. Esto es algo para tener en cuenta.

Caso práctico

Para corroborar esta interferencia se realizó una prueba dentro de un edificio en donde el access point no tenía ningún problema de cubrir el complejo por completo.
Es access point era un Cisco Airones 350 Series el cual inicialmente transmitía al máximo de 100mW. Como cliente wireless se utilizó una laptop con AirMagnet como software de seguridad. El horno microondas utilizado fue un LG-GoldStar el cual estaba ubicado en el break room de la empresa y el cual consumía 1.200 watts y funcionaba a 2.450 MHz, el cual está cerca del canal 9 de 802.11b.

Antes de encender el microondas se cambió el access point al canal 9 y se chequeó su rendimiento: 667 packets per second (pps). En el momento en el que el microondas estaba en pleno funcionamiento el rendimiento del access point descendió a 90pps, una disminución de más del 85 por ciento.

Esta es una considerable reducción de la performance, pero es la peor situación a considerar. El access point estaba en la misma frecuencia que el microondas, y no es probable que alguien utilice un cliente wireless tan cerca del aparato.
En cambio, si lo colocamos a dos metros y medio es una distancia un poco más realista. Ante esta situación su rendimiento fue de 178pps, lo que significa un descenso del 75 por ciento, número que a nadie pondría contento. Pero para entender qué significa hay que estar navegando en una página con algunos gráficos: mientras el microondas estaba

funcionando las imágenes cargaban muy despacio y hasta se corría el riesgo de congelar la carga total. En cambio, al apagar el microondas y borrar el caché del browser se pudo navegar sin ningún problema por las mismas páginas y de forma rápida.
Hasta a seis metros de distancia del microondas se continuaba experimentando algunas fallas.

Algo a considerar es que estas pruebas fueron realizadas con solo un cliente wireless activo, si hubieran habido más usuarios en la red los resultados hubiesen sido peores.

Como habrá visto, el horno microondas no derriba por completo la WLAN, pero sí es importante estar al tanto de la situación para que no nos tome desprevenidos. ●

¿Qué hacer respecto a la interferencia del horno microondas?

- Cambie el canal del access point. El horno microondas utilizado en el testeo no ocasionó demasiados problemas entre los canales 1 y 6. De hecho, el browser de la Web funcionó bastante rápido con el microondas funcionando y el acces point seteado en el canal 1 y canal 6. Tenga en cuenta que su horno microondas puede funcionar en una frecuencia diferente y no en la banda de 2.4GHz.
- Evite utilizar la WLAN cerca de un horno microondas. Manténgase a por lo menos un metro y medio del microondas cuando éste esté en uso mientras utiliza las aplicaciones de la WLAN.

La libertad de imprimir



Finalmente llegó y de la mano de Lexmark. La X4550 es la primera multifunción Wi Fi presentada en nuestro país y por esto fue la elegida de nuestro review. Ligera, rápida, fácil de usar y principalmente donde se quiera son algunas de sus características.







Características

La **Lexmark X4500** es una versión mejorada de la ya conocida X3550: con mejor performance pero con el mismo diseño y características. En cuanto al hardware tiene un peso total de 2,7 kg y un tamaño de 177 milímetros de alto, 453 de ancho y 325 mm de profundidad, un tamaño bastante adecuado si pensamos que al ser wireless se la puede ubicar en cualquier lugar.

Esta multifunción nos permite imprimir, copiar y digitalizar a través de los botones "Modo de Copia", "Modo de Escaneo" y "Tarjeta Fotográfica", los cuales su configuración puede variar según el modo en el que se esté trabajando.

Este dispositivo utiliza dos cartuchos de impresión, como la mayoría de las multifunción. Es bastante fácil de colocarlos o reemplazarlos y existen dos posibles configuraciones. La primera, y la más común, será utilizar el compartimiento izquierdo para el cartucho de color negro y el derecho para el de color (amarillo, cyan y magenta). En cambio, si lo que se busca es máxima calidad fotográfica se tendrá que sustituir el cartucho de tinta negra por otro específico de tres tintas, llamado "cartucho fotográfico".
Con respecto al software viene con dos CDs, uno para su instalación en Windows y el otro exclusivo para Macintosh. Incluye un manual en español y portugués bastante completo el cual indica cómo instalar la multifunción en cualquiera de los dos sistemas operativos. Vale recalcar que la instalación es bastante sencilla y se puede hacer vía USB o Wi Fi.

Performance

Una de las cuestiones que más importa a la hora de analizar una impresora es la relación costo/impresión; conocer la cantidad de hojas que imprime y cuál es la calidad de impresión respecto del precio tanto de la impresora como de los cartuchos.
En este sentido, la **X4550** no sobresale ni por su calidad ni por su velocidad de impresión. Pero si tenemos en cuenta que el costo total sugerido de esta multifunción wireless es de $699 (con IVA incluido) la relación costo/beneficio es más que aceptable.
La impresión de texto en blanco y negro tuvo una performance mejor de la que se esperaba y si bien al imprimir desde el Word se experimentó un retardo en la reacción, no se le quita puntos ya que la tinta no se corre y es bastante precisa la impresión.

En cuanto a velocidad la **Lexmark X4550** imprime hasta 15 páginas por minuto (ppm) en modo normal y negro y hasta 6 a color. Con respecto a la resolución, bastante importante a tener en cuenta, en negro fue de hasta 1200 x 1200 ppp y en color hasta 4800 x 1200 ppp.

Las MFPs (Multifunction Printers) son sin duda alguna la solución ideal para cualquier Pyme



como para el hogar. Cuenta con el beneficio de tener varias funciones en un mismo dispositivo, logrando de esta forma ahorrar en espacio y en costos, algo fundamental hoy en día.

Lo complicado de estas soluciones es encontrar una cuya performance sea excelente en cualquiera de sus funcionalidades. Si no se encuentra habrá que poner en la balanza cuál es el uso que más le vamos a dar y si vale la pena la inversión a realizar.

En cuanto a la **Lexmark X4550** su principal característica es la conexión Wi Fi, pero vale la pena si realmente se va a utilizar esta función. De todas formas, aunque en la actualidad no lo necesitemos, una multifunción es algo que seguramente no cambiemos por un par de años, y tenemos que tener en cuenta que en el futuro la característica de wireless nos puede ser de mucha utilidad.

En cuanto a la performance es bastante buena en lo que a impresión de texto se refiere. Si lo que se desea imprimir son fotografías conviene utilizar la opción de 6 tintas y el papel fotográfico Lexmark. Esta impresora puede resultar algo lenta, sobre todo a la hora de imprimir fotos, pero si se necesita una multifunción que cumpla bien en todas sus facetas para los quehaceres cotidianos, la X4550 es una muy buena elección. Y si tenemos en cuenta la relación costo/beneficio, no tendremos ninguna otra duda. •

Características Técnicas

- **Tecnología de impresión:** Inyección de tinta térmica.
- **Tecnología color:** Inyección de tinta en 4 colores: Cian, Magenta, Amarillo, Negro.
- **Impresión fotográfica** en 6 colores opcional.
- **Tecnología de digitalización:** CIS / CCD con 48 bits de profundidad.
- **Función:** Copia, Impresión, Digitalización en color.
- **Puertos estándar:** USB 2.0 Hi-Speed certificado USB pass through via puerto PictBridge.
- **Inalámbrico** 802.11g.
- **Rango de reducción/aumento:** 25 - 400 por ciento.
- **Área de digitalización**, Máxima (mm): 216 x 297 mm.
- **Tamaño (mm - Al x An x Pr):** 177 x 453 x 325 mm - 45 x 37 x 16 cm.
- **Peso (kg)**: 2,7 kg.
- **Ciclo de explotación máximo:** 3000 páginas por mes (una vez como máximo).

ELIGIENDO LA VIDEOCÁMARA PERFECTA

La variedad de formatos que utilizan los medios de comunicación y el surgimiento de la alta definición han hecho que comprar una cámara sea todo un reto. Aquí algunas claves para facilitarle la tarea.

El mundo de las cámaras de video está evolucionando rápidamente. Y si bien las ya clásicas cámaras basadas en el formato MiniDV aún ocupan un lugar importante en muchos hogares, las ventas de modelos que utilizan otros medios de grabación no paran de crecer. Los reproductores de DVD se han hecho tan omnipresentes en los hogares del mundo que la posibilidad de grabar videos directamente en ese formato es más que tentadora.

ABI Research, importante investigadora del mercado tecnológico, estima que para el año 2012 alrededor de un 50 por ciento de las cámaras de video grabarán en formato DVD o directamente en el disco duro, dato a tener en cuenta ya que éstas otorgan mucha mayor capacidad de almacenamiento.

Por tanto, la aparición de la alta definición y una constante disminución de tamaño y precio de los dispositivos ha otorgado la posibilidad de que cualquiera que pueda acceder a estas cámaras logre grabar videos con calidad profesional.

Conocer los formatos

Cada uno de los principales formatos en el mercado tiene ventajas específicas así como desventajas a las que se debe atender y conocer bien antes de realizar la compra.

Las cámaras basadas en Mini DV son de bajo costo, ofrecen muy buena calidad y la mayoría de los usuarios se encuentra familiarizado con su uso. Sin embargo la cinta se degrada con el tiempo.

Aquellas que utilizan tarjetas de memoria Flash, tienden a ser más pequeñas, livianas y por ende más portátiles y compactas, pero la capacidad de grabación suele ser algo limitada.

Las que graban en formato DVD cuentan con la comodidad de no tener que realizar ninguna conversión para la edición o almacenamiento en el formato estándar de estos tiempos, sin embargo no ofrecen la calidad o la capacidad de almacenamiento de otros modelos.

Por último las que graban en el disco duro otorgan una gran capacidad de almacenamiento pero la edición y el intercambio de imágenes puede resultar un verdadero desafío.

Alta definición vs. Definición estándar

En la actualidad una gran cantidad de las cámaras que se comercializan llevan las letras HD, High Definition, aunque muchas veces se trata de una estrategia de marketing publicitario y no de la realidad.

Para que una cámara sea efectivamente de alta definición, debe capturar imágenes con 1080 líneas de definición, más de cuatro veces más que las convencionales.

Entre las ventajas que las HD ofrecen se destacan un rango más amplio de colores, detalles que las otras cámaras no pueden capturar, y la grabación de imágenes "widescreen", lo que permite aprovechar todas las potencialidades de las pantallas de última generación.

Las consideraciones de diseño

La forma, el tamaño y el peso de las cámaras pueden resultar fundamentales a la hora de la elección.

Las cámaras flash pueden ser ideales para las personas con manos pequeñas mientras que se tornan incomodas para aquellos que tienen manos más grandes. También hay que tener en cuenta que a menor peso mayor probabilidad de que la cámara se mueva o tiemble si no se usa un trípode o base.

Por eso es fundamental elegir la cámara ideal para nuestras necesidades y capacidades.

Los sensores y CCD

Además del formato de grabación es muy importante tener en cuenta el sensor de luz integrado que poseen las cámaras. Algunas utilizan los chips CCD más antiguos, mientras que otras usan las nuevas obleas CMOS, que consumen menos energía aunque resignan algo de calidad.

Los sensores más grandes suelen ser mejores y más caros pero siempre depende de las necesidades de cada uno si vale la pena apostar por uno de ellos o utilizar los que la cámara ya trae incorporados.

Características

¿Qué más puede hacer la cámara? ¿Se le pueden agregar filtros y objetivos extras? ¿Cuenta con conexiones para micrófonos, auriculares, entradas analógicas y digitales? ¿Cuál es la autonomía de la batería?

ALTA DEFINICION

Permiten sacar el máximo provecho de los televisores de grandes pantallas y alta definición. Además otorga la posibilidad de capturar escenas sin perder el más mínimo detalle.

Características únicas

- Resolución de hasta 1080 pixels.
- Captura mayor cantidad de video utilizando menos espacio de almacenamiento que los otros formatos.
- Incluye una amplia gama de opciones de formato como DVD, MiniDV, Flash y Disco Duro.

Advertencias

- Un gran porcentaje de las cámaras que se promocionan como de alta definición, son en realidad cámaras de calidad estándar.
- Se necesita una computadora o laptop muy poderosa para editar video HD.
- No existen muchas opciones a la hora de elegir un software de edición HD.

SONY HDR-UX20

Ofrece tres formatos de grabación, DVD, memoria interna flash de 8 GB y Memory Stick PRO Duo, gracias a la nueva tecnología Hybrid Plus, que permite además una mayor flexibilidad a la hora de transferir las filmaciones y fotos.

Incorpora además sonido ambiental Dolby Digital 5.1, pantalla LCD, lente Carl Zeiss, estabilizador de imagen NightShoot, y todo lo necesario para realizar grabaciones de nivel profesional.



SONY HANDYCAM DCR-SR82

Con su disco rígido de 60 GB permite capturar hasta 14 horas de grabación en alta calidad. Posee una pantalla LCD de 2.7" en formato WideScreen y Zoom Óptico de 2000x. Ofrece también muy buen sistema de estabilizador de imagen y de grabación nocturna. Permite grabar imágenes fijas en Memory Stick.

DISCO DURO

Es ideal si usted no quiere tener que preocuparse del tiempo de grabación o del espacio de cinta. Con discos integrados que van desde 30 hasta 100 MB pueden capturar entre 5 y 14 horas de grabación.

Características únicas

- Se puede transferir grabaciones en video a la computadora de manera rápida y fácil para luego editar o grabarlo en DVD. Ofrece más tiempo de grabación que cualquiera de las otras cámaras y la comodidad de no necesitar tener una cinta de repuesto a mano.

Advertencias

- Se pueden tener problemas con la luz ya que algunas cámaras que graban en disco duro ofrecen incluso menos luminosidad que las Mini DV.
- Muchas HDD ofrecen sólo estabilización de imagen digital que es inferior a la estabilización óptica.

FLASH

Las cámaras que graban en tarjetas de almacenamiento extraíble han experimentado un rápido crecimiento y son muy populares entre los usuarios que gustan de compartir videos en línea.

Características únicas

- Una de las cámaras más pequeñas y ligeras.
- Las tarjetas de memoria se consiguen a precios cada vez más económicos.
- Permiten compartir videos en línea de manera sencilla y rápida. Ideal para los amantes de YouTube o sitios por el estilo.

Advertencias

- Al igual que muchas cámaras HDD, algunas de las cámaras que utilizan memoria flash tienen problemas de luz y un excesivo movimiento.
- Son especiales para publicar videos en la Web, pero no resultan tan competitivas para otros fines.

SANYO XACTI E1

Se trata de un interesante híbrido entre cámara digital y videocámara, disponible en una variedad de colores además de ser resistente al agua. Incluso el micrófono es capaz de capturar sonido bajo el agua. Ofrece una buena calidad de imagen VGA a 30 fotogramas por segundo y a 6 MP en imágenes fijas. Es capaz de capturar hasta 10 horas de video en una tarjeta SDHC de 8 GB.



DVD

Las cámaras de DVD representan el segmento de mayor crecimiento en este mercado y de a poco van reemplazando los modelos MiniDV como las preferidas de los usuarios y como la gran apuesta de los fabricantes. Sin dudas se trata de la videocámara de la década, más teniendo en cuenta que el formato DVD es el formato que se ha impuesto en el mercado del video.

Características únicas

- Permiten el placer de visualizar en cualquier reproductor de DVD las imágenes que recién se han registrado.
- Como se trata del sucesor del MiniDV estas cámaras cuentan con muchas de las características de diseño y extras a las que las Mini nos tienen acostumbrados.
- Requiere mucho menos espacio de almacenamiento que las cintas MiniDV.

Advertencias

- La mayoría de los disco DVD-R no permiten grabar nuevamente sobre cintas ya utilizadas.
- El polvo y los roces pueden dañar gravemente los discos.
- No siempre los fabricantes de cámaras DVD tienen en cuenta que sean compatibles con las interfaces de Mac o PC.

CANON DC 230

Se trata de un dispositivo sólidamente construido que otorga un fiable rendimiento de video, un zoom de largo alcance, resulta fácil de manejar y a un muy competitivo precio. Permite grabar aproximadamente una hora de metraje con un disco DVD R.



PANASONIC PV-GS85PL-S

Esta es una sólida cámara Mini DV, que brinda una gran calidad de video, incluso con poca luz. Ofrece una muy buena estabilización óptica y ranura para tarjetas SD. Además permite grabar video y foto simultáneamente.



MINI DV

Este formato si bien tiene unos cuantos años en el mercado aún se mantiene muy vigente. La familiaridad y confiabilidad son sus mayores atributos, además de su competitivo precio y el hecho de las cintas de grabación se encuentran disponibles en casi cualquier lugar.

Características únicas

- Como el formato más antiguo disponible, las videocámaras Mini DV han refinado a fondo sus características y a menudo pueden producir mejores imágenes que algunas cámaras que capturan en alta definición.
- Las cintas de Mini DV son compatibles con casi cualquier software de edición, lo que puede resultar una verdadera bendición cuando se edita.
- El convertidor analógico digital en cámaras Mini DV puede ser utilizado para digitalizar antiguas cintas de VHS.

Advertencias

- Transferir imágenes a una computadora lleva un tiempo. Si se trata de una grabación de 30 minutos, tardaremos 30 minutos en copiarla a la computadora, ya que realiza copias en tiempo real.
- Durante la transferencia de imágenes se pueden eliminar sonidos que presenten problemas de sincronización.



IDC Business Intelligence 2.0 Conference 2008

BUENOS AIRES, ARGENTINA: 10 de Junio - *Hotel Marriott*

SANTIAGO, CHILE: 03 de Junio - *Grand Hyatt*

business intelligence 2.0

Durante esta conferencia usted podrá conocer cuales son las principales tendencias de BI en Latinoamérica y el mundo.
Conozca las estrategias de las principales empresas del mercado, quienes estarán presentando un caso de éxito para mostrarnos cómo es BI en la práctica.



>> Speaker IDC: Alejandro Florean
Software Research Program Director Latin America

"En Momentos donde el entorno económico es volátil, las empresas deben de encontrar la menera mas eficiente de incrementar el ROI de la Información."



>> Chairwoman: Mariana Zamoszczyk
Senior Analyst, Software & IT Services IDC Argentina.

"En la actualidad, las empresas manejan un flujo de información que va en constante aumento, incrementado a su vez la complejidad de los procesos de toma de decisión. Por tal motivo, contar con herramientas de BI que permitan optimizar la performance del negocio en tiempo real se torna esencial. "

Para más información o registrarse:
>> ARGENTINA: conferencias_ar@idclatin.com | www.idclatin.com/argentina
>> CHILE: conferencias_ch@idclatin.com | www.idclatin.com/chile

Peligro para los niños en MUNDOS VIRTUALES

Las redes sociales para niños son hoy parte de Internet. Hoy los niños entran a sitios donde juegan e interactúan con otros miembros casi siempre comandando un personaje: por ejemplo un pingüino, ratón o dragón.

Autor: Dr. C. O. Rodriguez



En US existen sitios muy establecidos como Club Penguin de Disney (http://www.clubpenguin.com), Neopets (www.neopets.com) y Webkinz (www.webkinz.com). Estudios recientes hablan de 12 millones de niños y teens online en US y 20 millones para 2011 en este tipo de redes.

Estos mundos virtuales son en general gratuitos y tienen publicidad de productos de quienes patrocinan el sitio o de terceros. Y aquí radica uno de los problemas: muchos expertos en privacidad están preocupados por el marketing invasivo y la cantidad de información que estos sitios reúnen y cómo será utilizada. En US las leyes y legislaciones vigentes son muy claras en este sentido. Aún así existen zonas grises muy peligrosas.

ENTENDIENDO EL PROBLEMA

El mercado para los niños

Jeff Chester es director ejecutivo del Center for Digital Democracy (www.democraticmedia.org). Jeff explica que "uno está hablando de sitios con entornos interactivos diseñados específicamente con un propósito que plantean desafíos fundamentales al desarrollo psicológico único y vulnerable de un niño. No son terrenos virtuales movedizos en los que se mueven estos marketineros: es hielo real muy fino".

Esto se mezcla a otro debate, el problema de "depredadores" que siempre está presente en el tema de niños online.

En el caso de US y Europa las leyes que protegen de sitios web invasivos tratan de incluir a los padres en el circuito. Para acceder a un sitio para niños, teniendo menos de 13 años, es indispensable tener un consentimiento "verificable" de los padres. Muchas veces es solo exigido un email de los padres y por tanto un niño puede fraguarlo muy fácilmente.

El sitio www.wiredsafety.org está dedicado a esta problemática. Su director Parrym Aftab es un abogado especializado en privacidad en Internet y comenta que "algunos sitios solo dicen 'este es un sitio sólo para gente mayor de 13 años, así que si no los tiene, vaya a otro lugar' y de este modo liberan al sitio de responsabilidad aun cuando el sitio es atractivo a menores de 13".

Algunos sitios como el popular Neopets, sin embargo, aseguran que mantendrán la información recogida sobre gustos y preferencia de los niños en forma confidencial siempre y cuando el niño quede dentro de su sitio. Si por un link pasa a otro sitio, existirá otra

Center for Digital Democracy

El CDD, fundado en 2001, se dedica a garantizar que el interés público sea una parte fundamental del nuevo paisaje de las comunicaciones digitales. Desde abrir las redes de banda ancha, el acceso gratuito a Internet o de bajo costo, a la diversidad de la propiedad de nuevos medios de comunicación, a la intimidad del consumidor, el CDD trabaja en la promoción de un sistema de medios de comunicación electrónica que fomente la expresión democrática y de derechos humanos. Como grupo sin fines de lucro, con sede en Washington, DC, el CDD trabaja para estar en la vanguardia de los nuevos medios de comunicación, especialmente con un seguimiento de los mercados comerciales de comunicación. A través de la divulgación, fomenta el desarrollo de comunidades en línea y servicios esenciales para la sociedad del siglo XXI.

Links de redes sociales de niños

www.panfu.es
www.clubpenguin.com
www.neopets.com
www.webkinz.com
www.haboo.es

"Algunos sitios solo dicen 'este es un sitio sólo para gente mayor de 13 años, así que si no los tiene, vaya a otro lugar' y de este modo liberan al sitio de responsabilidad aun cuando el sitio es atractivo a menores de 13".

política de seguridad sobre la cual ellos no tienen responsabilidad.

Valerie Steeves es profesora de la Universidad de Ottawa, Canadá y experta en temas de derechos humanos y tecnología y explica que "si uno mira a Neopets es claramente un sitio divertido donde jugar. Pero en realidad es una empresa de investigación de mercado. El disclaimer dice algo como: 'además estamos aquí para coleccionar su información personal y venderla y ver modos de conocer sus comportamientos' pero esta información está sumergida en párrafos legales en algún lugar donde el niño muy probablemente nunca llega".
Analicemos como ejemplos de políticas las de uno de los sitios populares. Club Penguin de Disney es claro en que no compartirá la información ni mostrará ningún tipo de publicidad... excepto quizás algunos de sus productos. El hecho de que cobra para poder acceder hace que no necesite (en principio) tener que ganar por publicidad. Existen sin embargo algunas cláusulas muy debatibles.

Alguien al acecho que se hace pasar por niño en los chats y sus peligros

El peligro de depredadores sexuales está siempre latente en los chats de sitios para niños. Algunos sitios y sus mundos virtuales son relativamente seguros en este sentido. Se ofrecen servicios de chat muy restringidos donde los niños solo pueden usar diálogos pre-definidos. Si ofrecen la posibilidad de diálogos más amplios se busca el consentimiento de los padres, se utilizan filtros y moderación en vivo de modo de mantener las cosas dentro de normalidad.

Y como tercera posibilidad relacionada a mayores mal intencionados aparece el cyberbullying (intimidación) y cyberstalking (acecho).
Sumado a los motes más comunes de harrassment (acoso) y llamado de nombres ofensivos los niños muchas veces roban passwords y toman control de la cuenta de otro deleteándola o usándola con fines maliciosos. Aftab comenta que a pesar de las medidas que se toman en este sentido (aun con niños llamados agentes secretos que ayudan) ella sabe de varios incidentes de suicidio de niños relacionado a este tipo de problema.

Haboo (www.haboo.es) es un sitio muy popular con los niños donde este fenómeno es muy común y donde se utilizan con éxito moderadores de sitio junto a filtrado.

Las pregunta que me hago es si existen leyes similares en Argentina. ¿Y son aplicadas? Espero poder responder esto en un próximo artículo resultado de una investigación que estoy realizando. •





Nuevos modelos de negocios: NUEVOS DESAFÍOS

Dos noticias diferentes son una muestra bastante acabada de lo que está sucediendo cada vez más frecuentemente en nuestra industria IT y aledaños: los modelos de negocios alternativos a los tradicionales están asomando la cabeza y volviéndose cada vez más una opción razonable.

Durante mucho tiempo, Metallica, la banda metálica más poderosa del planeta (según sus fans, por supuesto) se erigió en uno de los más importantes combatientes de la música por Internet y, más específicamente, de la posibilidad de bajar música de la Red, de cualquiera de las maneras posibles. Léase tanto legal como ilegal.

En línea con organizaciones como la RIAA, que agrupan a las grandes compañías discográficas, Lars Ulrich, el vocero de la banda, insistió en categorizar como piratería cualquier intento de compartir música en la red. Se respeten o no los derechos de autor, o se discuta si el intercambio de PC a PC en forma gratuita constituye, verdaderamente, un acto de piratería.

La noticia de semanas atrás (1) dice que, siguiendo el ejemplo de Radiohead y Nine Inch Nails, "Metallica está planeando un release digital para su próxima producción". Más aún, estarían dispuestos a permitir que los fans compren MP3 de su discografía e, incluso, podrían bajar gratuitamente viejos shows.

Por el otro lado, el 24 de abril pasado, en conmemoración del Día Mundial de la Propiedad Intelectual (que se "celebra", en realidad, el 26 de abril), se coordinó un panel con representantes de las distintas organizaciones que conforman la Organización Mundial de la Propiedad Intelectual (OMPI) en la Argentina. A excepción de uno de los integrantes (el director Juan José Jusid), el resto de los panelistas y el mismo presentador eran más bien representantes de las organizaciones administradoras de las creaciones, antes que creadores, como se refleja en esta nota de Tecnozona (2).

La gran uniformidad de las exposiciones se vio quebrada ante la insistencia de gente del público que proponía debatir modelos de negocios alternativos a los tradicionales de "protección de la propiedad intelectual" como eran llamados. La negativa a tratar esos temas fue bastante concreta. Algún asistente recordó que en un panel semejante pero del año pasado, había participado un diseñador de juegos que, al proponer una salida alternativa como Creative Commons, había sido "fusilado" por la representante de Argentores, a la sazón una de las principales defensoras del sistema actual que esta vez estaba entre el público. El actual modelo de negocios de la cinematografía, de los videojuegos, de la música y las discográficas y, por supuesto, del software, está en crisis. Y en este caso, en crisis no significa necesariamente en caída sino en revisión, en crítica.

Internet, las nuevas tecnologías digitales (¿cómo distinguir el original de la copia cuando ambos son idénticos?) y de comunicaciones (incluyendo GPRS/EDGE y 3G) han puesto en tela de juicio la validez y la persistencia de modelos de negocios basados en otros soportes y, sobre todo, en otros conceptos distintos de la propiedad intelectual, para usar un término genérico. No debemos olvidar que en el ambiguo concepto de "propiedad intelectual" entran los derechos de autor, las patentes, las marcas registradas, las licencias, etc.

Lo concreto es que la noción de "piratería" sólo es concebible en un determinado contexto, en un modelo de negocios específico. En el software libre, por ejemplo, la piratería no existe, no es posible. Sin caer en los extremos fundamentalistas, tanto del mercado como del software libre (de los fundamentalistas del software libre, GPL, Creative Common y otras licencias "libres", aclaremos), lo cierto es que hoy en día coexisten distintos tipos de licenciamientos que admiten diversos modelos de negocios: la venta de los "derechos de uso" o la suscripción a servicios de soporte, para citar dos ejemplos típicos. Y es importante que tengamos la mente abierta no sólo para aceptar su existencia sino también para darnos cuenta de que, en una de esas, a lo mejor, también uno de ellos puede ser nuestro modelo de negocios. ●

(1) http://blog.wired.com/music/2008/04/metallica-consi.html
(2) http://www.tecnozona.com.ar/modules/AMS/article.php?storyid=1495

■ **Ricardo D. Goldberger**
Periodista Científico especializado en Informática y Nuevas Tecnologías

Autor: José Jaliff

JEE vs .NET

Una comparativa entre dos grandes para el desarrollo de aplicaciones empresariales.

Con el presente artículo trataremos de aclarar algunas dudas sobre estas dos plataformas de desarrollo empresarial que cada vez tienen más adeptos.

En principio muchos suelen confundir y comparar JAVA con .NET, lo cual no es correcto teniendo en cuenta que JAVA es un lenguaje de programación mientras que .NET es una plataforma de desarrollo para aplicaciones empresariales. Por lo antes dicho es que se hará una comparativa entre JEE y .NET no solo a nivel estructura, sino también en otros aspectos que pueden ser interesantes para mencionar.

Comencemos con una breve explicación de ambas plataformas para luego entrar en detalle con la comparativa de las mismas.

.NET

La plataforma Microsoft .NET (ver figura 1) es una plataforma de desarrollo la cual consiste en un conjunto de aplicaciones y servicios de empresa. La compilación, al igual que sucede con Java, se realiza en dos pasos sucesivos. El código escrito por el programador se compila en el lenguaje intermedio de Microsoft (MSIL: Microsoft Intermediate Language). Es entonces cuando el CLR (CLR: Common Language Runtime o entorno común de ejecución) de Microsoft compila en tiempo de ejecución las aplicaciones en código nativo de la plataforma. El CLR también revisa el código, verificando la seguridad y recolectando los objetos para los cuales no existe ya ninguna referencia (recolección de basura), además de gestionar las excepciones entre otras tareas. Es inevitable notar que en este punto .NET tiene muchas similitudes con JEE.

La tecnología .NET no se basa en un solo lenguaje de desarrollo, sino que se pueden utilizar distintos lenguajes en un mismo entorno. Para garantizar que esto ocurra, es necesario que los lenguajes usados cumplan la CLS (Common Language Specification), una especificación de los tipos de datos, estructuras y operaciones comunes a todos los lenguajes de programación o lo que es lo mismo, un subconjunto del CTS (Common Type System).

JEE

La plataforma de desarrollo JEE es, según Sun Microsystems, más que una plataforma, es un conjunto de estándares y especificaciones para el desarrollo de aplicaciones empresariales basado en la tecnología y lenguaje Java.

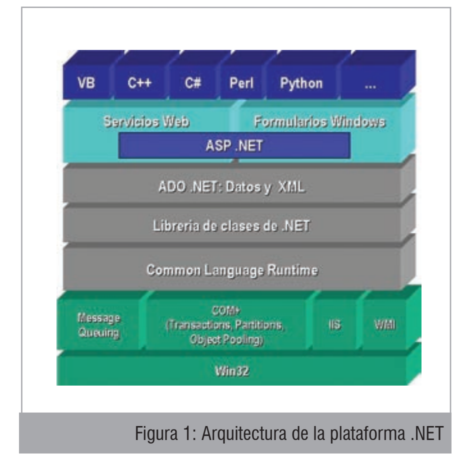


Figura 1: Arquitectura de la plataforma .NET

La plataforma JEE ha sido creada con la participación de cientos de empresas de diversa índole y es por lo que no podemos decir que es únicamente de Sun su autoría. Actualmente se han desarrollado una serie de herramientas de todo tipo pero no todas son de Sun e incluso muchas son Open Source.

El lenguaje en el que se basa JEE es Java, un lenguaje orientado a objetos que ya lleva muchos años en el mercado por lo que logró alcanzar su madurez. Tanto es así que hoy en día en el ámbito académico está reemplazando al clásico C++. La expansión de este lenguaje entre la comunidad de programadores ha sido también muy vertiginosa y se ha impuesto más que como un leguaje orientado a objetos, sino que JAVA es un lenguaje de objetos.

JAVA es un lenguaje de programación neutral, portable, estable, independiente de la plataforma, sencillo de aprender ya que la mayoría de los programadores en la actualidad programó o programa en lenguajes orientados a objetos. JAVA se hizo fuerte sin duda por ser independiente de la plataforma por lo que se pueden realizar aplicaciones multiplataforma real (para Linux, Windows o para sistemas operativos para ordenadores personales o estaciones

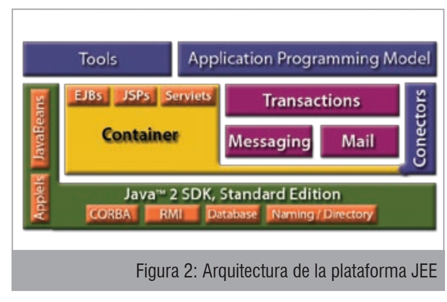
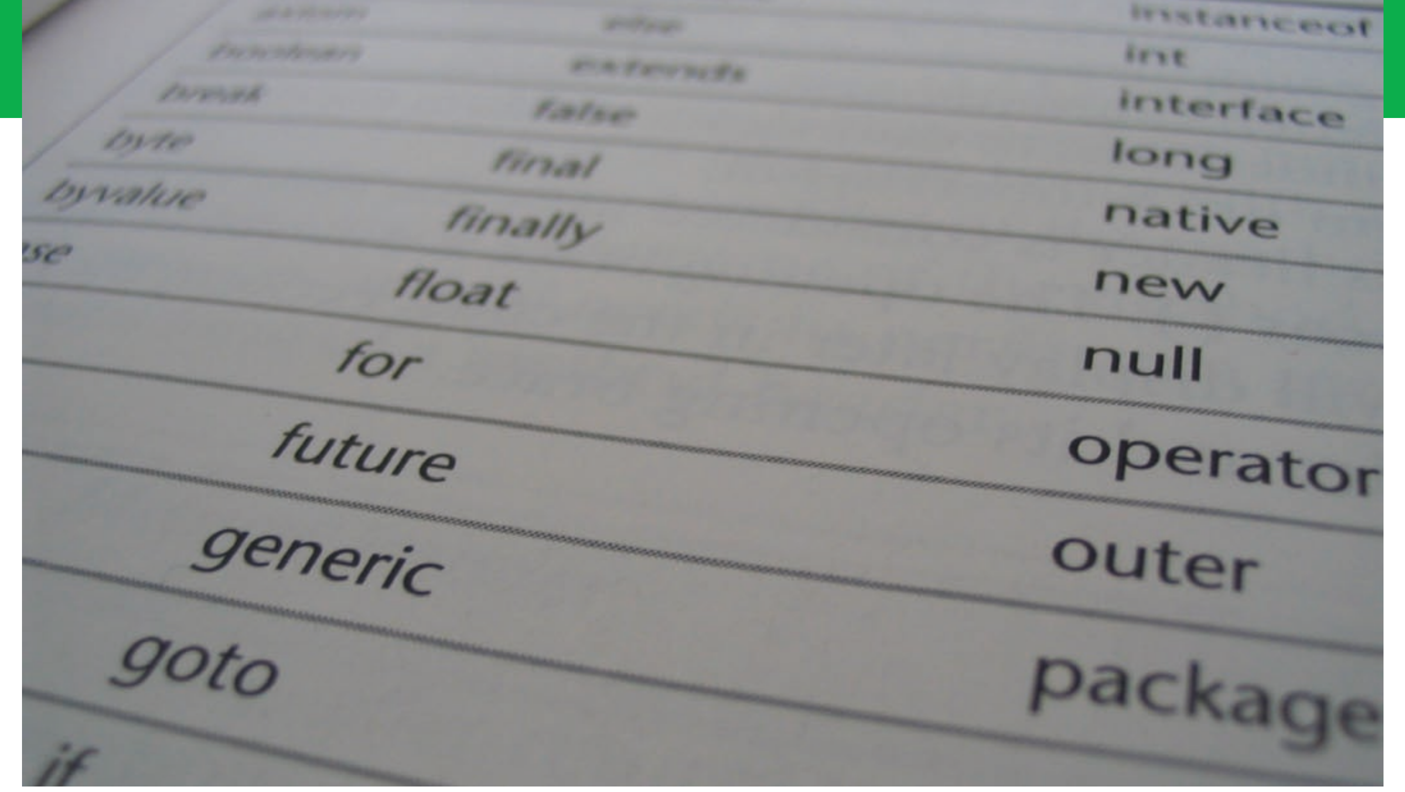


Figura 2: Arquitectura de la plataforma JEE



www.sxc.hu - Chris

de trabajo, y Palm OS o EPOC, como así también entre muchos sistemas operativos para dispositivos de telefonía móvil).

Al estar la plataforma JEE basada en el lenguaje JAVA, se garantizan la portabilidad gracias a que la aplicaciones no se compilan en código específico para la máquina en la que se ejecutará, sino que se transforma en un conjunto de bytecodes independientes de la plataforma utilizada que son leídos e interpretados por la máquina virtual Java (JVM) para ejecutar el programa (ver figura 2).

Semejanzas entre JAVA y C#

Antes de entrar en la comparativa de ambas plataformas de desarrollo es conveniente enumerar algunas de las semejanzas entre el lenguaje JAVA y el lenguaje C#.

- Ambos lenguajes compilan un código independiente de la máquina y el sistema operativo que se ejecuta mediante sus correspondientes entornos (JVM o entorno .NET).
- Incorporan un "recolector de basura".
- No necesitan punteros (Java no los permite y C# permite un uso restringido dentro del código señalado como unsafe, inseguro).
- No se utilizan ficheros de cabecera (como en C y C++), todo el código se empaqueta en packages (Java) o assemblies (C#).
- Admiten hilos (threads).
- Admiten herencia múltiple mediante interfaces.
- Permiten clases internas (clases en el interior de otras clases).
- No admiten programación estructurada, no se pueden colocar métodos sueltos, todos tienen que estar dentro de una clase.

Comparativa estructural

- El propósito tanto de JEE como de la plataforma .NET es facilitar y simplificar el desarrollo de aplicaciones empresariales o corporativas. De cara al comercio electrónico, las JSP (Java Server Pages) son muy similares a las ASP (Active Server Pages) o a las nuevas ASP .Net, y los EJB (Enterprise JavaBeans) son muy similares a los COM/COM+ de Microsoft.
- Los servidores de aplicaciones J2EE y .Net proporcionan un modelo de acceso de componentes a datos y de lógica del negocio, separados por una capa intermedia de presentación implementada mediante ASP .Net (.NET) o Servlets (JEE).
- Visual Basic .Net y C# son lenguajes orientados a objetos, al igual que Java.
- Desde la perspectiva de los desarrolladores, JEE y .Net proporcionan las herramientas para crear fácilmente Servicios Web.
- Tal y como se ha expuesto, JEE y .Net son multiplataforma. Al usar .Net una compilación en dos pasos, le permitiría teóricamente proporcionar entornos de ejecución para diferentes plataformas de forma similar a Java y sus JREs y SDKs.

Ventajas de .NET frente a JEE

a) Una ventaja muy importante del entorno .Net frente a JEE es la posibilidad de emplear múltiples lenguajes de programación, mientras que JEE sólo trabaja con uno: Java. Aunque sin duda algún teórico pensará que lo ideal sería que solo hubiera un lenguaje de programación (a ser posible estandarizado). La realidad es que esta alta diversidad de lenguajes es obligatoria por la misma variedad de las necesidades de los programadores. Todavía hoy existen más líneas de código escritas en Cobol que en C++ o Java. Un lenguaje moderno y orientado a objetos como Java puede resultar totalmente ineficaz -y hasta inadecuado- a la hora de abordar problemas que involucren cálculos matemáticos masivos y complejos, mientras que esos mismos cálculos pueden ser abordados mucho más adecuadamente con un lenguaje tan primitivo. Por otro lado, .Net posibilita así que programadores de terceros lenguajes pasen a esta plataforma reduciendo el tiempo de aprendizaje y entrenamiento.

b) Las herramientas de desarrollo incluidas por Microsoft en su Visual Studio .Net son mucho más simples, intuitivas y sencillas de manejar que las herramientas de desarrollo equivalentes en JEE suministradas por otras empresas (o por Sun). Cualquier programador medio/avanzado se manejará rápidamente con la programación del interface de usuario en Visual Studio .Net, al igual que sucedía con versiones anteriores de Visual Studio.

c) C# es un lenguaje interesante, fácil de on el presente artículo trataremos de aclarar algunas dudas sobre estas dos plataformas de de

El propósito tanto de JEE como de la plataforma .NET es facilitar y simplificar el desarrollo de aplicaciones empresariales o corporativas. De cara al comercio electrónico, las JSP (Java Server Pages) son muy similares a las ASP (Active Server Pages) o a las nuevas ASP .Net, y los EJB (Enterprise JavaBeans) son muy similares a los COM/COM+ de Microsoft.

aprender por los programadores de Java (de hecho, Microsoft ofrece un conversor de Java a C#), que en caso de estandarizarse podría resultar un lenguaje muy conveniente para ciertas tareas de programación en diferentes plataformas. No está escrito en ninguna parte que los lenguajes no puedan evolucionar y, en ese sentido, C# es una rama evolutiva más del árbol de los lenguajes orientados a objetos.

d) Microsoft ha impulsado con gran energía los servicios Web y ha resaltado su importancia entre toda la comunidad de desarrolladores. La plataforma .Net se ha diseñado considerando los servicios Web (mientras que JEE no) siendo estos servicios propios de la plataforma y ofrece una nueva versión de ASP, ASP .Net, que puede considerarse un entorno de programación "de verdad" en lugar de un entorno basado en scripts. Microsoft .Net fue construido para la integración a través de los servicios Web XML usando protocolos y formatos de ficheros como SOAP (Simple Object Access Protocol), WSDL (Web Services Description Language) y UDDI (Universal Description, Discovery, and Integration). Comparativamente, .Net va por delante con respecto a JEE con respecto a servicios Web y estos servicios son propios de la plataforma, aunque JEE tampoco se queda atrás solo que es más complejo trabajarlos, la facilidad, rapidez y sencillez con la que se pueden construir servicios Web con el Asistente de servicios Web de Visual Studio .Net son muy superiores a las de las herramientas para construir servicios Web dentro del entorno de JEE.

Ventajas de JEE frente a .NET

a) Las implementaciones de JEE pueden adquirirse a distintas compañías, mientras que .Net solo puede comprarse a Microsoft.

El hecho de que haya distintas organizaciones implementando JEE ofrece mayor variedad para los usuarios finales y permite la existencia de una cierta competencia entre ellas para obtener mejores productos, lo que no existe en el caso de Microsoft y su .Net.

b) Debido al proceso evolutivo de los productos de Microsoft, y en muchos casos, por motivos de compatibilidad, la seguridad frente a virus informáticos de los productos de Microsoft es menor que los basados en Java, pues desde un comienzo Java se fundamentó en un estricto modelo de seguridad.

c) Como se ha dicho anteriormente, las aplicaciones Java pueden correr en una amplia gama de sistemas operativos y de arquitecturas de hardware. Hasta la fecha, .Net no tienen una independencia real de la plataforma, siendo JEE el único entorno de desarrollo que ofrece una independencia real de la plataforma.

d) La tecnología Java es una tecnología abierta (en el sentido de que el código de la plataforma completa puede ser obtenido, revisado y estudiado por cualquiera que esté interesado) y se basa en gran parte en estándares de organizaciones de normalización y estándares empresariales. Esto posibilita que los desarrolladores puedan conocer y entender completamente cómo hace las cosas en Java y aprovecharlo para sus aplicaciones y, por otro lado, al basarse en estándares empresariales, simplifica la integración con productos de múltiples compañías. En contraposición, solo el código fuente del Nuevo lenguaje C# de la plataforma .Net ha sido abierto al público general (aunque Microsoft permite a compañías con las que le unen intereses comunes el acceso al código fuente de ciertas partes de .Net).

e) Aunque Java fue creado originalmente por una compañía, Sun MicroSystems, lo cierto es que JEE es ahora el producto de la colaboración de más de 400 empresas y organizaciones de todo tipo (públicas, privadas sin ánimo de lucro, privadas con ánimo de lucro y de normalización en ámbitos nacionales e internaciones). La plataforma .Net es -y será- el producto de una sola compañía, que aunque haya implementado algunos estándares en .Net y esté intentando conseguir que ciertas tecnologías se conviertan en estándares "oficiales", no puede tener el mismo consenso que .Net (sobretodo teniendo en cuenta que la mayor parte de su código no es público).

f) La tecnología Java goza ya de una cierta veteranía (más de 10 años en el mercado). JEE y ha probado su eficacia en muchos entornos y situaciones empresariales distintas, mientras que .Net le falta más tiempo de demostrar.

Mundo laboral

Según lo que he podido ver en mi vida laboral, y lo que he hablado con muchos colegas y empleadores del sector, los programadores JEE cobran más caro el valor de sus conocimientos. Esto puede ser una gran ventaja para los programadores que manejen esta plataforma, del mismo modo que para los empleadores puede llegar a ser una desventaja. Por este mismo motivo es que cada vez más programadores prefieren estudiar JEE para garantizarse un mejor sueldo en el mercado laboral.

A pesar de todo esto, JEE gana en el terreno del desarrollo de aplicaciones empresariales por su madurez, ya que lleva muchos más años que .NET en este tipo de desarrollos, aunque .NET se va acercando poco a poco. Teniendo esto en cuenta podemos ver que en las ofertas laborales del sector informático la gran mayoría de los avisos tanto en Internet como en diarios y otros medios están destinados a programadores para la plataforma JEE.

En conclusión, antes de decidir qué plataforma de desarrollo se va a utilizar para un determinado proyecto, se deberían analizar todas y cada una de las ventajas y desventajas mencionadas, para que el equilibrio costo/calidad sea el más favorable. ●

Acerca del autor

José Jaliff es líder técnico en una importante multinacional de sistemas especializado en tecnología JAVA y gerente de AbyssKey, empresa con la que realiza Consultoría y Desarrollo de Software para la Argentina y el exterior.



6 de Mayo

Sheraton Libertador. Av. Córdoba 690.

A partir de las 9.00 hs.



TENÉS EL TRABAJO QUE QUERÉS?

ANDÁ IMPRIMIENDO TUS CURRICULUMS.

Estudiantes, profesionales y representantes de los departamentos de Recursos Humanos de empresas líderes reunidos bajo un mismo techo. Propuestas laborales, útiles conferencias, todos los tips para buscar trabajo y desarrollar una carrera laboral existosa en la Argentina de hoy y del mañana.

Las mejores empresas te van a estar esperando



Inscribite gratuitamente

www.jornadatrabajoit.com.ar

y comenzá a participar de las búsquedas de estas importantes empresas.



ORGANIZA



IMPULSA









INFORMES: WorkTec Argentina, Tel.: +54.11.4706.3000. info@worktec.com.ar









jobs steve

Renaciendo de las cenizas

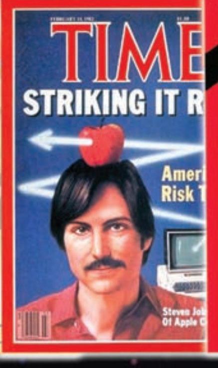
Es sinónimo de innovación, rebeldía y diseño. La manzana representa su imperio. Amado por algunos por renacer de las cenizas y odiado por otros por su carácter déspota, Steve Jobs, CEO de Apple Computer y de Pixar Animation Studios, se lleva el crédito por haber creado y recreado a una de las empresas que más da que hablar en la actualidad: Apple.















Steve Paul Jobs nació el 24 de febrero de 1955 en San Francisco pero fue dado en adopción de inmediato con la única condición de que sus padres adoptivos le garantizaran una educación universitaria. De esta forma, su familia pasó a ser Paul y Clara Jobs, una humilde pareja que vivía en donde al poco tiempo se lo conocería como Silicon Valley.

A los 11 años Steve descubrió el mundo de la electrónica junto a su vecino Bill Fernandez y a Steve "Woz" Wozniak, cinco años mayor que él, con quien al tiempo participó del desarrolló de un dispositivo llamado blue box, el cual permitía realizar llamadas internacionales de forma gratuita. Esta fue su primera aproximación a la tecnología. Pero no la última.

Al terminar el secundario, Jobs siguió el mandato de sus padres biológico y asistió al Reed College en Oregon, una de las universidades de mayor prestigio en los Estados Unidos. Sin embargo, luego de un par de meses de intensas clases, Steve empezó a cambiar el foco de su interés: de la Física y Literatura Inglesa pasó al misticismo.

"Luego de seis meses no le encontraba el sentido. No tenía ni idea lo que quería hacer con mi vida ni cómo la universidad me ayudaría a saberlo. Y allí estaba yo, gastando el dinero que mis padres habían ahorrado durante toda su vida. Así que decidí renunciar y confiar que todo se iba a salir bien. Tuve mucho miedo, pero fue una de las mejores decisiones que tomé en mi vida, dejé las materias obligatorias y comencé a cursar las que realmente me interesaban. De todas formas no todo fue romántico. No tenía un lugar en donde dormir por lo que me quedaba en cuartos de amigos, juntaba botellas de gaseosas y por cada una obtenía 5 centavos que los usaba para comprar comida y caminaba 11 kilómetros todos los sábados para tener una comida decente a la semana en el templo Hare Krishna. Lo amé".

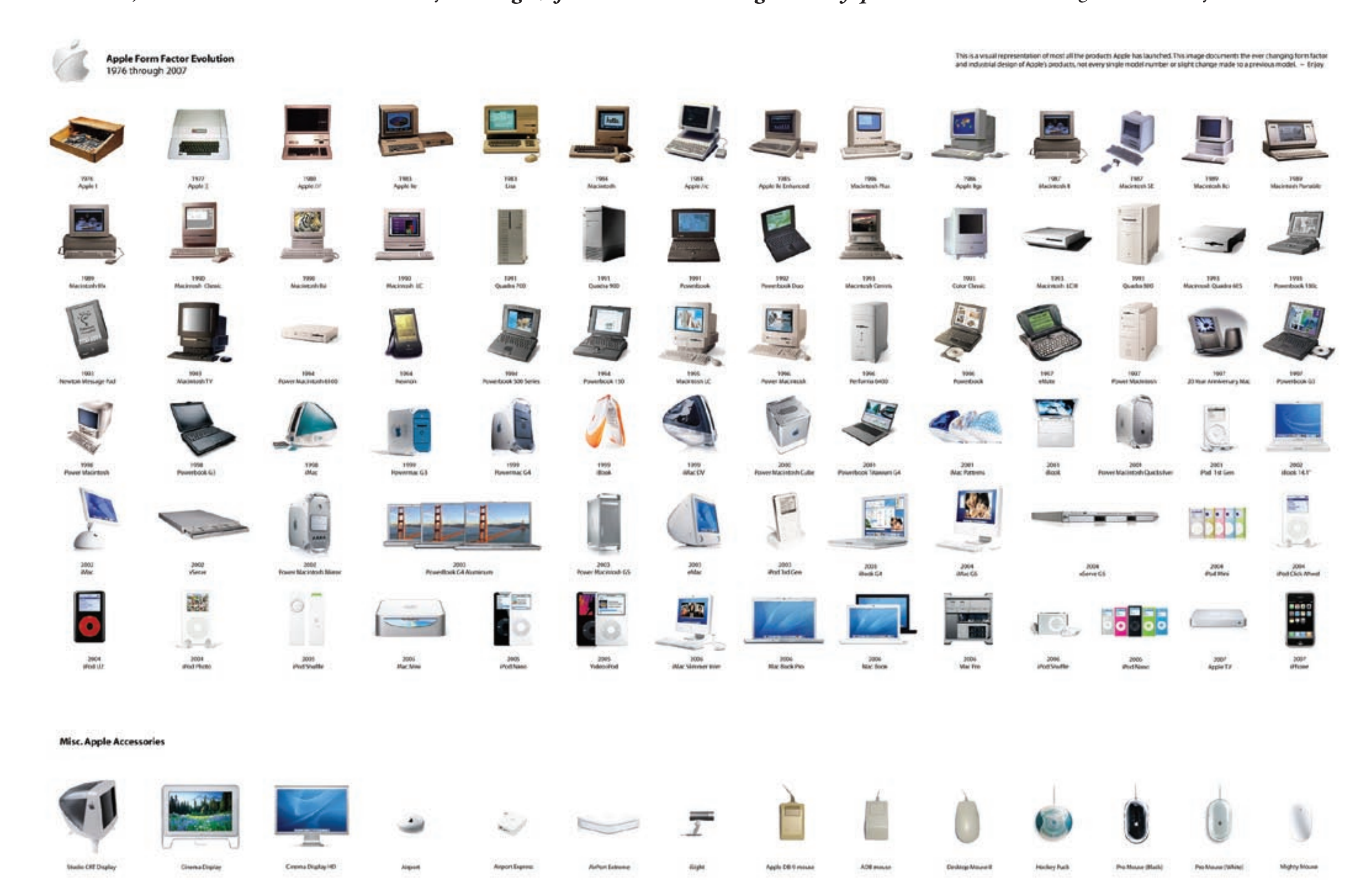
Ya en 1974, con apenas 19 años de edad y sin rumbo fijo, Steve logra su primer trabajo en Atari, una incipiente pero exitosa empresa de video juegos que estaba experimentando un gran crecimiento. Sin embargo este logro no lo convenció y luego de un fracasado viaje por la India en busca de respuestas, encontró lo que necesitaba de la mano de su amigo Woz. Nuevamente se volvió hacia la electrónica al descubrir que existía todo un mundo detrás del diseño de una computadora personal compacta.

"Muy poca gente estaría interesada en construir una computadora personal, pero sí muchos estarían desesperados en usarla para programar". Con esta afirmación nació Apple Computer en abril de 1976. El nombre fue elegido por un conjunto de razones, entre ellas que la manzana era la fruta favorita de Steve, quien en ese momento era frugívoro.

¿El capital inicial? Bastante modesto: $500 de una van Volkswagen de Steve y $500 más de una calculadora HP de Woz.

La primera venta vino de la mano de un retailer local: The Byte Shop, quien compró 50 computadoras Apple a $500 cada una. La primera de ellas fue ensamblada en el garaje de los padres de Steve en Los Altos, con un par de amigos dispuestos a ayudar.

Para ese momento ya se estaba diseñando la Apple II, la cual cargaba automáticamente su sistema operativo y no necesitaba de un ventilador (que Steve odiaba) gracias a un revolucionario suministro eléctrico. Pero por sobre todo, podía realizar un mayor número de tareas que las de sus competidores con un menor número de componentes.



Luego del rotundo éxito de la Apple II, de una fuerte inversión en la empresa por parte de Mike Markkula, un retirado ejecutivo de Intel, y del nombramiento de Mike Scott como presidente, Steve comenzó a trabajar en su próximo proyecto: Lisa. Su principal atracción era una innovadora interfaz gráfica para el usuario (GUI) con un escritorio con ventanas, carpetas y la posibilidad de cortar y pegar. Sin embargo, y a pesar de sus ganas de estar al frente de su proyecto, Jobs fue nombrado Chairman de la Junta Directiva. Gracias a su talento y carisma, el reconocimiento masivo se hizo evidente el 12 de diciembre de 1980 cuando Apple realizó una oferta pública de ventas: Steve Jobs se convirtió en el multimillonario más joven de los Estados Unidos con una fortuna de $217.5 millones de dólares.

Pero Jobs no se sentía cómodo en su lugar de Chairman y prefería involucrarse en el desarrollo de los productos de la empresa de la manzana. Inmediatamente formó un equipo de trabajo para desarrollar Macintosh, una computadora basada en la idea de simplicidad y más pequeña y barata que Lisa, pero incluyendo sus características gráficas.
El pequeño grupo que conformaba el equipo Mac mantenía un espíritu rebelde alentado por el propio Jobs: los ingenieros del proyecto se veían así mismos como "Piratas" y se referían al resto de la compañía como "la Marina". En 1984 Macintosh fue lanzada al mundo pero sin el éxito esperado: era un poco lenta y tenía muchas dificultades para correr software empresarial.

Para ese entonces, la relación entre Jobs y el CEO de la compañía, John Sculley, iba de mal en peor y cada uno de los miembros de la Junta Directiva votó a favor de la remoción del fundador de Apple Computer.
"A los 30 ya estaba afuera. Y de forma pública. Lo que había sido el foco de mi vida entera ya no estaba, y era devastador. Realmente no sabía qué hacer en los próximos meses. Me junté con David Packard y Bob Noyce e intenté disculparme por haber cometido tantos errores. Y realmente fui una decepción pública, hasta pensé en mudarme. En su momento no lo vi, pero el haberme ido de Apple fue lo mejor que me podía haber pasado".
Luego de un período que incluyó un viaje a París, Suecia y la USSR, en septiembre de 1985 Steve funda, junto a otros cinco ex empleados de Apple, la empresa NeXT Computers, con el objetivo de crear una computadora exclusiva para el mercado de la educación superior.

Pero el serio problema de distorsión de la realidad de Steve nunca estuvo tan acentuado como durante la existencia de NeXT. Todo el mundo se preguntaba acerca del revolucionario producto en el que Jobs y su equipo estaba trabajando, y la política de secreto era tan estricta que hubo un silencio extremo durante tres años completos. Durante todo ese tiempo, el cebo para atraer a nuevos empleados no era el trabajo en sí, sino Steve mismo. El ir a trabajar para NeXT implicaba dedicar la vida entera a una empresa, sin saber exactamente en qué se iba a trabajar. Steve Jobs utilizó su extraordinario carisma para de esta forma contratar a los mejores talentos, y como no podía ser de otra forma, utilizó métodos poco convencionales: "Uno debía conocer básicamente a todo el staff y lograr la aprobación de cada uno de ellos para poder ingresar a la compañía. Se sentía más como una fraternidad. Todos tenían que quererte. Y es por esto que el sentimiento que uno tenía era que debía ser 'el mejor de los mejores' para poder entrar".

Pero el progreso de NeXT como empresa era realmente lento. No solo se buscaba la computadora perfecta, sino un sistema operativo acorde que lo acompañara: NeXTSTEP, basado en un estable y poderoso SO desarrollado por universitarios, UNIX. Sin embargo, este sistema operativo no incluía la interfaz gráfica de la Mac y se le sumaba el revolucionario diseño (como el de un cubo) que, si bien le daba mucha elegancia al modelo, los costos de manufactura fueron diez veces más altos que los pensados originalmente.

A pesar de varios intentos de revertir la situación y convertir al cubo en un computador más accesible, en 1993 Jobs se vio obligado a dejar de lado el desarrollo del hardware y enfocarse en NeXTSTEP. Desde ese momento Steve comenzó a dejar de lado la vida pública y a refugiarse en su familia.
La realidad de Steve parecía llevarlo otra vez al fracaso público, pero una inversión que había realizado años atrás lo salvaría de la ruina y lo devolvería al podio.

En 1986 Jobs había comprado la división Industrial Lights & Magic de George Lucas por 10 millones de dólares y al momento la incorporó como Pixar Animation Studios, la cual estaba formada por un pequeño gru-



po que creían fielmente en la animación computada. Realmente no obtenían fuertes ganancias y lo único que frenó el cierre de Pixar fue la nominación al premio de la Academia como Mejor Film Corto Animado en 1986 por Luxo Jr. y en 1989 al Oscar por Tin Toy.
En 1991 Jobs firma un acuerdo con Disney para coproducir la película animada Toy Story, gracias a la cual, en 1995 pasó de tener un capital de $11.2 millones de dólares a estar de vuelta en la cima con $420 millones.

Pero mientras Steve Jobs estaba en su mejor momento, Apple perdía presencia en el mercado y debía salir a luchar contra un nuevo enemigo: Microsoft. Por tanto, la empresa de la manzanita decide a fines de 1996 la compra de NeXT Software Inc. para poder hacerle frente al Windows NT.
Steve había vuelto y más fuerte que nunca. Como parte de la Junta de Directores comenzó a tomar medidas drásticas para intentar salvar a la compañía: canceló decenas de proyectos y redujo costos desde donde se pudo. En 1998 Steve anunció que Apple arrojó, por primera vez en 10 años, ganancias.
Pero lo mejor aún faltaba: en mayo de 1998 se lanzó al mercado la iMac, una elegante y colorida computadora cuyo diseño evocaba a la Macintosh original. ¿El resultado? Fue un éxito rotundo, Apple volvió a estar en el centro de la acción y Steve Jobs volvió a ocupar su lugar original: el de CEO de su propia empresa.

En 2001 Apple logró dar con la clave y apoderarse del trono: lanzó el Mac OS X 10.0, la primera versión de un sistema operativo desarrollado sobre NeXSTEP y con una revolucionaria interface llamada Aqua, y el primer iPod.
Lo que viene después es historia conocida para todos nosotros: una sucesión de éxitos empezando desde el iTunes, pasando por el Mac OS X y llegando al revolucionario iPhone.
No hay dudas de que Steve Jobs encontró la forma de renacer de las cenizas y volver a la cima. Durante toda su vida se ha enfrentado a grandes dificultades pero logró superarlas satisfactoriamente: ha sido humillado, traicionado por sus colaboradores más cercanos y hasta se ha enfrentado a la muerte cuando, en 2004 le diagnosticaron un raro tipo de cáncer de páncreas y tuvo que ser intervenido quirúrgicamente. En la actualidad es una de las figuras más prominente en el mundo de la tecnología y hasta fue nombrado en 2007 por la revista Fortune como el hombre de negocios más influyente del mundo por su activo rol en la industria de la computación, de la música, la animación y los teléfonos.

Sin embargo, muchos niegan su habilidad de ver hacia dónde se dirige la industria tecnológica y le han atribuido su éxito a una cuestión de mera suerte: estar en el lugar adecuado en el momento preciso. Sin embargo la Macintosh, Pixar, el iPod, el iPhone y el hecho de que las tres empresas que fundó hayan sido reconocidas como símbolos de vanguardia y de innovación da para pensar.

¿Suerte? Puede ser. ¿Carisma? Seguro. Pero especialmente una gran cantidad de talento y empuje de un hombre que nunca ha dejado de impresionar al mundo y que no está dispuesto a frenar. ●



NOTA #3 - Serie "Redes de Acceso"

Autor: Miguel F. Lattanzi
Ing. en Telecomunicaciones (IUPFA)

FOTO: http://www.sxc.hu/ Marco Soscia



implementación de ADSL

En las redes de acceso por banda ancha intervienen varios componentes bien diferenciados, tanto a nivel de protocolos de comunicaciones como de equipamiento de red. Veremos, con un enfoque práctico, cómo es que todos estos componentes interactúan entre sí para poder brindar los servicios de acceso a los usuarios finales.

En el presente artículo de la serie "Redes de Acceso" daremos un paso al costado con los temas teóricos que vinimos desarrollando y en cambio daremos un giro hacia una aplicación práctica, describiremos cómo se establece un servicio de ADSL (Asymmetric Digital Subscriber Line), extremo a extremo, desde el equipo del abonado o CPE (Customer Premises Equipment) hasta el borde de la red del proveedor de servicios.

Describiremos los protocolos que intervienen en el establecimiento de la conexión y en la transmisión de los datos y explicaremos las principales características de los equipos que intervienen en la red de acceso.

Descripción General y Topología

El conjunto de equipos necesarios para poder brindar un servicio de acceso de datos a alta velocidad (extremo a extremo) está compuesto por tres grupos principales de dispositivos: los equipos del usuario –o abonado–, los equipos de la red de acceso del proveedor y los equipos del borde de la red principal, también del proveedor de servicios.
Todos estos equipos pueden ser vistos en la figura 1. A continuación veremos una breve descripción de cada uno:

CPE
Son los equipos de los usuarios, para el caso de las redes xDSL son ni más ni menos que MODEM (MOdulator-DEModulator) xDSL.
Estos moduladores-demoduladores son los que se encargan de transformar las señales digitales provenientes de los equipos de los abonados (como ser una PC, un teléfono IP, etc.) a señales que puedan ser interpretadas por los DSLAM (Digital Subscriber Line Access Multiplexer).
Como se mencionó anteriormente, en los MODEM los usuarios finales conectan los equipos que tienen en sus casas, principalmente los equipos utilizados son PCs.
Estos equipos y los MODEM se interconectan, típicamente, por medio de un cable de red UTP (Unshielded Twisted Pair), aunque algunos MODEM más nuevos tienen capacidad de acceso inalámbrico utilizando Wi-Fi como tecnología de transmisión, ya sea por medio del estándar IEEE 802.11b (11 Mbps) o 802.11g (54 Mbps).
Aquellos que utilizan cable UTP soportan los estándares IEEE 802.3 y 802.3u. El primero se utiliza en redes cuya tecnología de transmisión es Ethernet y la capacidad de envío de datos es de 10 Mbps, el segundo establece una capacidad de hasta 100 Mbps.
La gran mayoría de los MODEM que soportan Wi-Fi también tienen puertos fijos Ethernet para conexionado por cable de red.

DSLAM
Es el primer equipo de la red del proveedor de servicios, es un equipo de acceso por par de cobre que utiliza la última milla de la red telefónica conmutada.
Existen básicamente dos tipos de DSLAM,

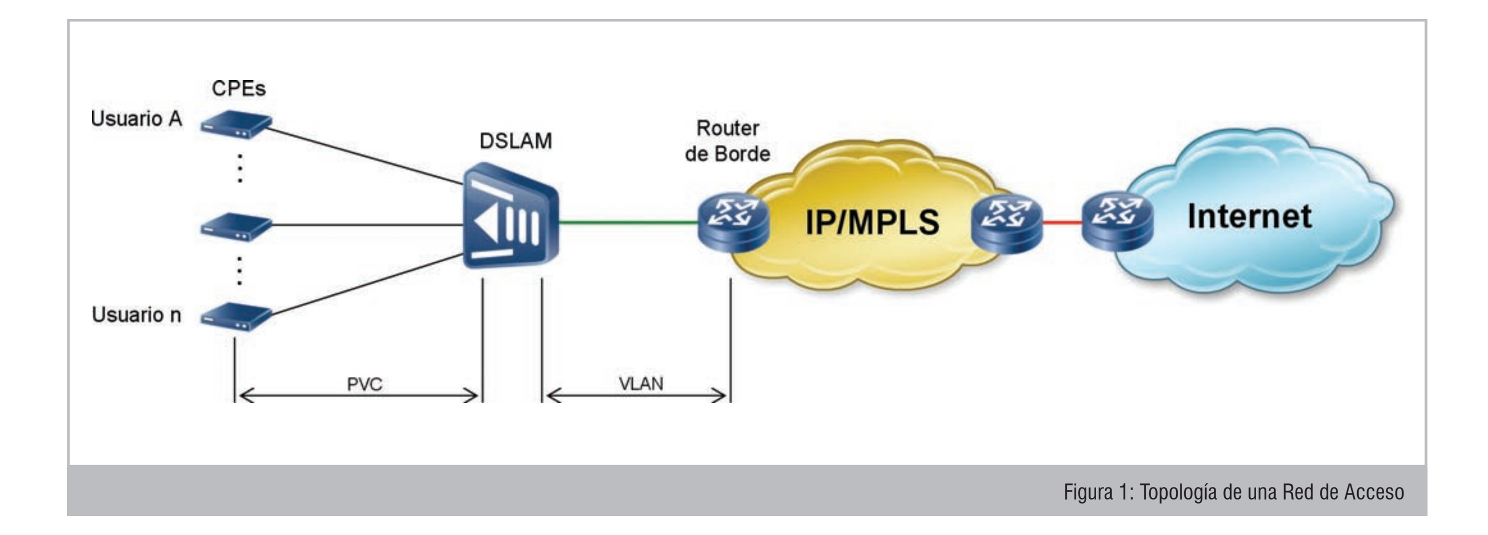


Figura 1: Topología de una Red de Acceso

ATM (que se conectan a una red ATM) y los IP que se conectan a una red Ethernet/IP, estos últimos son los más utilizados.

La salida de los MODEM de los abonados hacia el exterior de los hogares se realiza por el par de cobre ya existente para el uso del teléfono común (referirse a los artículos #1 y #2 de la serie Redes de Acceso para obtener más detalles técnicos).

Cada abonado tiene un puerto dedicado en el DSLAM, es decir que por cada abonado existente hay un par de cobre que se extiende desde la interfaz ADSL del MODEM (ATU-R) hasta la interfaz ADSL del DSLAM (ATU-C).

El DSLAM se encarga principalmente de concentrar en forma física a los diferentes usuarios, realizar una conversión de protocolos entre la red de acceso y la red WAN (Wide Area Network) y conmutar internamente el tráfico proveniente de los abonados hacia la red del proveedor de servicios.

Concentra físicamente, dado que los DSLAM tienen varios puertos de acceso por par de cobre, la concentración típica actual ronda los 1.000 abonados por equipo.

Realiza una conversión –o adaptación– de protocolos porque a nivel de capa dos del modelo de referencia OSI (Capa de Enlace de Datos) se utiliza el protocolo ATM (Asynchronous Transfer Mode) para encapsular los datos y enviarlos entre el CPE del usuario y el DSLAM.

Pero hoy en día, la tecnología más utilizada en los puertos troncales –o Uplink– está basada en Ethernet, mas precisamente en Gigabit Ethernet (estándar IEEE 803.2z).

Se puede observar, entonces, la problemática de tener ATM en el acceso al DSLAM y Ethernet nativo en el lado de red.

Para solucionarlo, el DSLAM procesa todas las celdas ATM que llegan a las interfaces de acceso ATU-C y retira la información del payload, esta información (que por lo general es Ethernet/IP) puede ser luego retransmitida sin problemas al equipo superior de la red, en este ejemplo básico sería el router de borde.

Con respecto a la funcionalidad de conmutación interna, el DSLAM utiliza PVC (Permanent Virtual Circuit) ATM para establecer los canales de comunicación hacia los CPE y VLAN (Virtual Local Area Network) hacia la red del proveedor.

Internamente el DSLAM asocia los PVC de los abonados con VLAN, entonces, una vez procesada la información del payload de las celdas ATM, se toma la trama Ethernet y se le coloca una o dos etiquetas de VLAN, según corresponda y sea la topología utilizada, para luego ser enviada por la interfaz Gigabit Ethernet.

ROUTER DE BORDE

El ER (Edge Router) se encarga principalmente de realizar funciones de autenticación de usuarios y terminación de sesiones punto a punto (contra el CPE), pero usualmente también se encargan de tareas de control de sesiones para facturación y de la administración del ancho de banda de los abonados.

Hay varias formas de encapsular el protocolo IP para poder establecer una comunicación entre los equipos del usuario y la red de telecomunicaciones, y acceder así al servicio deseado, por ejemplo Internet. Se debe tener en cuenta que sin importar si el protocolo IP será encapsulado sobre Ethernet o no, siempre la capa 2 entre el CPE y el DSLAM será ATM, con lo cual todos los métodos contemplan el uso de dicho protocolo.

Los métodos posibles son:

RFC 1483: Describe dos métodos diferentes para enviar tráfico de datos sobre una red ATM. Las variantes son RFC 1483R (Routed) y RFC 1483B (Bridged).

PPPoE: Point-to-Point Protocol (PPP) over Ethernet permite encapsular protocolos de capa 3 del modelo de referencia OSI (Capa de Red) sobre tramas PPP y estas a su vez sobre tramas Ethernet, para finalmente ser encapsuladas sobre celdas ATM (este método a veces es referenciado como PPPoEoA).

PPP es un protocolo de túnel que permite transportar protocolos como IP manteniendo los atributos de un enlace PPP punto a punto; como ser autenticación, encriptación y compresión.

Definición de VLAN

Son redes virtuales identificadas por una o dos etiquetas (campos) que se agregan en la trama Ethernet, el tráfico dentro de una VLAN se comporta como si se tratara de una red física. Por lo general se nombra a la primera etiqueta de VLAN como C-VLAN (Customer VLAN) y a la segunda como S-VLAN (Service VLAN). IEEE 802.1Q define la estructura de una etiqueta de VLAN e IEEE 802.1ad lo hace para el caso de dos etiquetas.

¿Por qué PPP?

Las redes Ethernet están basadas en la conmutación de paquetes y no soportan el concepto de conexión o circuito. Utilizando el protocolo PPP se puede hacer que los usuarios generen un “circuito” a través de una red Ethernet, estableciendo así una conexión punto a punto entre el CPE y el router de borde, que además permite funciones de autenticación al ser generada y luego permite enviar el tráfico de datos en forma segura.

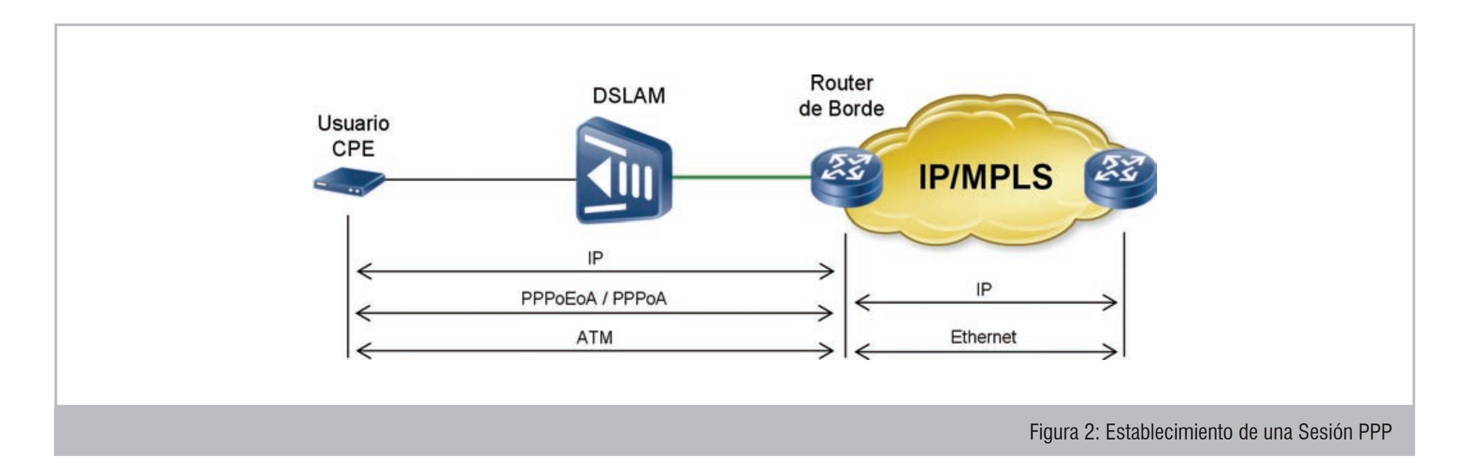
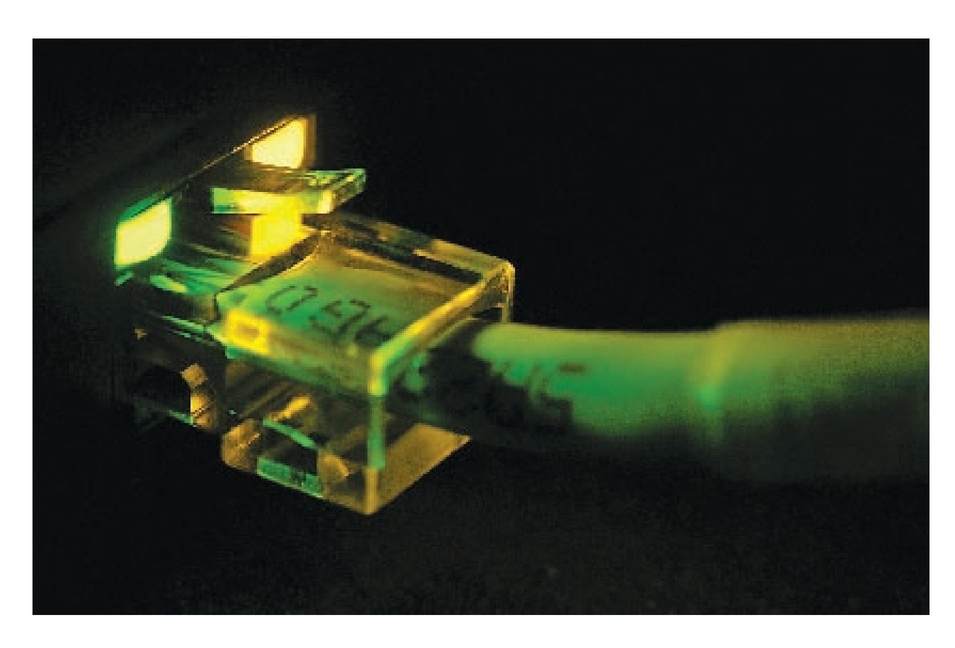


Figura 2: Establecimiento de una Sesión PPP

FOTO: http://www.sxc.hu/ Ozan Uzel



PPPoA: Point-to-Point Protocol over ATM es utilizado para encapsular los paquetes IP sobre tramas PPP y estas a su vez sobre celdas ATM, sin utilizar Ethernet previamente como en el caso anterior.

En función de las definiciones dadas anteriormente se puede analizar porqué el protocolo PPP es el elegido a la hora de establecer los servicios de acceso a Internet, principalmente por un tema de seguridad y autenticación.
PPPoE (o PPPoEoA) es el más utilizado debido a la ventaja de transportar las tramas Ethernet.
Los otros métodos de acceso englobados en RFC 1483 suelen ser utilizados por otro tipo de servicios que no requieran de autenticación o de la particularidad de un enlace punto a punto entre el equipo terminal del abonado y los equipos de la red del proveedor de servicios.

Ejemplo de Acceso a Internet

Para poder clarificar todos los conceptos dados y ver cómo es el establecimiento de una conexión típica de acceso a Internet veremos los pasos siguientes suponiendo que se utiliza el método de PPPoEoA:

1. El usuario "disca" o genera una conexión PPP desde su PC por medio de un software.
2. Entra en funcionamiento el protocolo PPP y tras intercambiar la información necesaria con el router de borde (ente otros datos el nombre usuario y password) se establece la sesión punto a punto. Aquí es donde el usuario obtiene la dirección IP de WAN que utilizará para el servicio de Internet.
   Todos los datos viajan encapsulados en paquetes IP que se encapsulan en tramas PPP y en tramas Ethernet y finalmente en celdas ATM. El direccionamiento aquí se realiza a través de los PVC. El DSLAM descarta las celdas ATM y retransmite las tramas Ethernet, con los protocolos PPP e IP, hacia el router.
3. Autenticado el usuario y verificados sus privilegios, el router comenzará a enrutar todos los paquetes IP a través de la red IP/MPLS (en este ejemplo) hacia un router con salida a Internet, el cual a su vez retransmitirá todos los paquetes a dicha red.
4. Cuando el usuario desea finalizar la conexión, se desconecta a través del software que genera la sesión PPP y ésta es liberada.
5. Por último el router también libera tanto la sesión de su interfaz como la dirección IP (que podrá ser reutilizada por otro usuario), permitiendo de esta manera que el usuario se conecte sin problemas en la próxima sesión.

Conclusión

Vale aclarar que este ejemplo es bastante básico pero sirve para ilustrar y dar una idea de cómo funciona un servicio de acceso por banda ancha, y sirve como punto de partida para profundizar tanto los conceptos relacionados con las tecnologías que intervienen en la red de acceso, como con los protocolos utilizados para el establecimiento del servicio.
En el próximo artículo de la serie de Redes de Acceso, Fibra Óptica en el Acceso, se desarrollarán los diferentes tópicos involucrados en las redes de acceso por fibra óptica.
Se hará una breve descripción de éstas, se diferenciarán los tipos existentes, los protocolos utilizados y las topologías que se suelen implementar. •

Notas de la Serie

#1 Evolución en el Acceso

#2 Tecnologías xDSL

#3 Implementación de ADSL

#4 Fibra Óptica en el Acceso

#5 Tecnologías xPON

Parte I de 4

Autor: Diego Javier Kreutzer
Ingeniero en Electrónica
(Univ. Nacional de La Matanza)

Voz sobre IP

[Inicio, objetivos y requerimientos]

Hace ya más de una década se comenzó a hablar de Voice over IP como una tecnología emergente para aplicaciones domésticas. Hoy, ya con la madurez necesaria, aparece como una solución corporativa escalable y de bajo costo. A lo largo de esta serie de 4 artículos veremos sus inicios, su presente y su tendencia de cara al futuro.

Un poco de historia

A comienzos de la década del 90, el mercado de las telecomunicaciones tenía su fuerte en el servicio de telefonía corporativa. Los accesos digitales (líneas TDM dedicadas) permitían al usuario instalar su propia PABX (Private Automatic Branch Exchange, también conocida como PBX) y de esta forma armar su propio plan de numeración de internos, tarifación y otras funcionalidades ofrecidas por la "centralita"; esta solución también aseguraba una muy buena calidad en la comunicación basada en la asignación fija de ancho de banda, siendo generalmente circuitos E1 o T1. Las llamadas de larga distancia representaban más del 10 por ciento del total de los minutos que facturaban las Telcos, por lo que la estrategia se basaba en ofrecer el minuto tanto local como de larga distancia a menor precio que la competencia. Por otro lado, y sin demasiada relevancia, los datos se transportaban vía modem a través de la PSTN siendo algo adicional a la transmisión de voz y muy poco utilizado; este escenario puede verse ejemplificado en la figura 1.

Ya a mediados de dicha década, la realidad de las empresas era muy distinta: el acceso a Internet y la transmisión de datos entre sucursales se habían convertido en una necesidad dejando relegado en importancia al servicio de telefonía corporativo. Se plantea entonces un nuevo escenario: se necesita una red de datos, pero que conviva con la red de telefonía; o bien, que ambos servicios puedan converger en una única red encapsulando el tráfico de voz en paquetes de datos.

Haciendo análisis de tráfico, los ISP tenían una alta demanda por parte de los usuarios durante la noche, mientras que el tráfico de voz (dominado por las Telcos) tenía su pico durante las horas del día; con los primeros indicios de voz encapsulada en 1996, los ISP se convierten en proveedores de voz y datos con la misma infraestructura. Frente a este panorama y viendo el emergente mercado de voz y datos unificados, las Telcos se vieron obligadas a cambiar su estrategia y comenzar a invertir en tecnología para lograr una infraestructura que les permitiera competir con los ISP.

La transmisión de telefonía a través de Internet tuvo gran repercusión a nivel doméstico debido a la alta densidad de hogares conectados y los bajos costos asociados; permitía llamadas de larga distancia a costos extremadamente bajos frente a una llamada telefónica de las mismas características, pero la calidad del tráfico sobre Internet era muy variable y esto representaba una limitación para ofrecer telefonía corporativa. En tales casos, las Telcos aprovechaban los enlaces dedicados para datos, sobre los cuales podían aplicar políticas de QoS y transmitir voz sin mayores inconvenientes (ver figura 2).

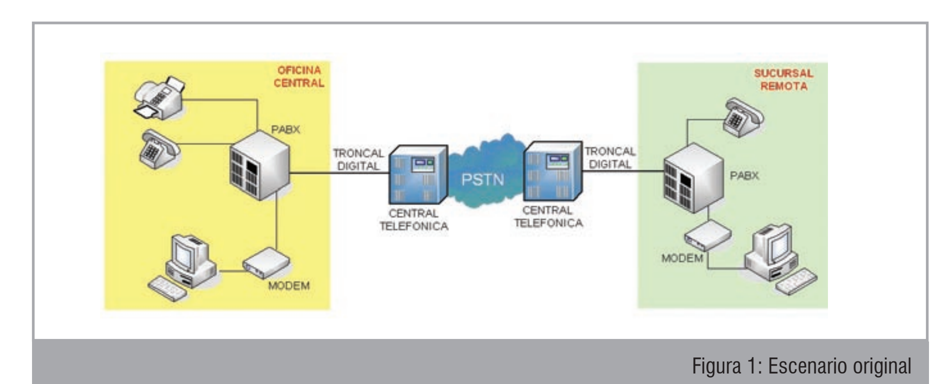


Figura 1: Escenario original

VoIP frente a VoATM y VoFR

Al igual que en redes IP, se puede transmitir tráfico de voz sobre redes ATM; estas últimas aseguran QoS debido a que son orientadas a la conexión y ofrecen mayor velocidad gracias al menor trabajo de procesamiento (celdas de igual tamaño), dando excelentes resultados. Sin embargo, IP tiene una mayor presencia frente a ATM (utilizado principalmente como backbone) y ofrece una diferencia más que significativa en costos de equipamiento.

También puede traficarse voz sobre redes Frame-Relay; es una tecnología madura, simple y fácil de implementar. Muchos carriers ofrecen servicios de datos sobre sus redes FR dando muy buenos resultados, pero es una estructura rígida y difícilmente integrable con otras tecnologías de Layer 2. Es en este punto donde IP marca la diferencia: a pesar de no ser orientado a la conexión y no tener un manejo innato de QoS, posee la particularidad de hacer converger las diversas tecnologías de la capa de enlace como IEEE 802.X, FR, PPP y ATM en una única capa de red de aplicación masiva, permitiendo implementar VoIP sobre cualquiera de ellas o bien, sobre MPLS (ver Redes MPLS y VoIPoMPLS en NEX IT Specialist #28).

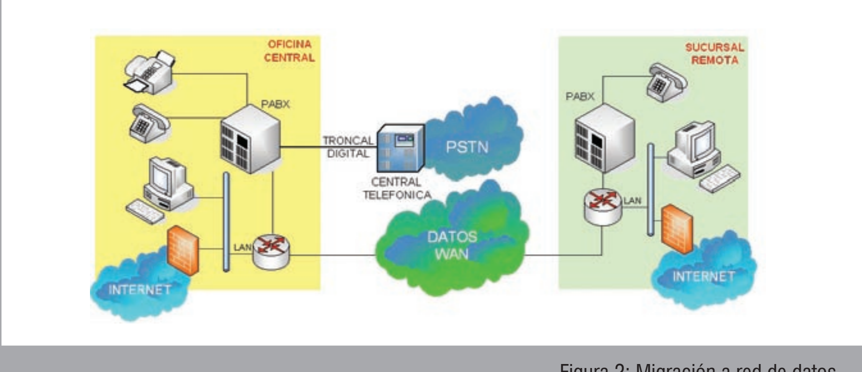


Figura 2: Migración a red de datos

Consideraciones acerca de VoIP

Como su nombre lo indica, VoIP (Voice over IP) es una tecnología que consiste en transmitir la voz encapsulada en paquetes IP, sobre la misma infraestructura en que se transmiten los datos. Las primeras aplicaciones estaban orientadas a utilizar la propia PC como una extensión telefónica y permitían comunicarse con alguien en otro extremo de la red; dependiendo del ámbito donde se da la comunicación aparecen otro tipo de productos como ser Voz sobre Internet o Telefonía sobre IP (ToIP), de la cual hablaremos en los siguientes artículos de la serie.

Ahora bien, ¿cuáles son las ventajas de transmitir voz encapsulada en IP? ¿Qué objetivos se persiguen? Veamos algunos puntos claves en respuesta a estas preguntas:

- **Utiliza IP:** TCP/IP es hoy en día la suite de protocolos más popular, tanto para redes privadas como para Internet; se encuentra presente en computadoras personales y es fácilmente configurable por el usuario.
- **Optimización de recursos:** en una conversación normal, aproximadamente el 56 por ciento de la misma está formada por pausas en el habla. En el esquema de conmutación de circuitos (telefonía convencional), esto significa un desperdicio importante del ancho de banda para los proveedores del servicio. Con un esquema de conmutación de paquetes, si se eliminan la información redundante y los silencios, puede manejarse como tráfico por ráfagas dando un mejor aprovechamiento de la red, ampliando la cantidad de comunicaciones por canal y permitiendo a los proveedores manejar flexiblemente los precios ofrecidos. Veremos en la próxima edición técnicas de compresión que permiten bajar la tasa binaria del canal telefónico digitalizado a menos de 64 kbps con una calidad apropiada.
- **Costos:** si analizamos la figura 2 puede verse que la sucursal remota prescinde de la PSTN para conectarse con el otro extremo y, por lo tanto, será como si llamada se realizara desde la oficina central. El tráfico de voz entre sucursales sobre la red de datos se traduce en un ahorro más que significativo en los gastos de telefonía pero siempre se debe mantener vínculos con la PSTN ya que la presencia de POTS aún hoy es mucho mayor que la de terminales de VoIP.
- **Infraestructura unificada:** tanto datos como como voz se trafican sobre una única infraestructura, facilitando la operación y el mantenimiento de la red y reduciendo la diversidad de equipamiento y de proveedores de tecnología.
- **Integración:** facilita el agregado de servicios adicionales como audio de alta calidad, videoconferencia, correo, mensajería unificada, etc.
- **Interoperatividad entre redes:** Permite conectar la red VoIP con la red telefónica convencional (POTS) y la red celular.

Sin embargo, transmitir voz implica tener en cuenta ciertos parámetros de calidad para obtener un resultado satisfactorio y comparable con el servicio tradicional.

Veamos algunos aspectos a considerar:

- **Delay (o retardo):** es el tiempo que transcurre desde que la voz parte desde el emisor hasta que llega al receptor. Según la norma G.114 de la ITU-T, el delay máximo admisible para una buena calidad de la señal vocal es de 150 milisegundos, restringiendo el acceso del tipo satelital cuya principal debilidad es el alto retardo. El delay está conformado por una parte fija y una parte variable; la parte fija se compone de:
  - **Delay de propagación:** depende del medio de transmisión (fibra óptica, cobre, radioenlace, etc) y no es percibido por el oído humano, pero sumado al resto influye sobre la calidad de la señal.
  - **Delay de serialización:** tiempo que demanda enviar el paquete a una interfase (store & forward o cut-through).
  - **Delay de procesamiento:** es el tiempo que se demora en el procesamiento de la voz, incluyendo digitalización, compresión y empaquetado de la señal. Esto será ampliado en el próximo artículo de la serie.

  Los siguientes componentes conforman la parte variable del delay:
  - **Delay de encolado:** demora ocurrida al colocar los paquetes en colas de espera debido a la congestión de la red.
  - **Delay por tamaño de paquete variable:** al tratarse de paquetes de longitud variable, puede ocurrir que el envío de un paquete de gran tamaño demore un paquete de voz.
  - **Delay por almacenamiento en buffers:** se utilizan buffers a fin de compensar el jitter, lo cual es explicado a continuación.
- **Jitter (variación del retardo):** este parámetro es la variación en el retardo de un paquete que va desde emisor al receptor frente al retardo de un paquete anterior (ver figura 3). Si todos los paquetes tardan el mismo tiempo en ir de un punto al otro, tenemos un jitter de 0 mseg. Su efecto es perceptible y molesto para el receptor.
- **Eco:** la reflexión de la señal eléctrica (que genera el eco en el audio) es el producto de desadaptación de impedancias en los cir-

cuitos de la central telefónica o del aparato telefónico. Se puede corregir utilizando canceladores de eco.

- **Pérdida de paquetes:** las redes de datos admiten pérdida de paquetes descartados por congestión o por errores; para un tráfico en tiempo real como la voz, esto afecta en gran medida la calidad de la comunicación ya que la retransmisión fuera de secuencia no sirve para subsanar la pérdida de un paquete intermedio.
- **Compresión:** debido a que los enlaces WAN son de baja velocidad, veremos más adelante que la voz se digitaliza y comprime a velocidades inferiores a los 64 kbps descartando los silencios generados durante la conversación y otra información redundante. El algoritmo a utilizar debe evitar la eliminación de componentes fundamentales de la señal ya que no posible recuperarlos en el receptor.
- **Factores psicológicos:** existen mecanismos que permiten detectar los silencios en la conversación y dejar de transmitir paquetes cuando la señal cae por debajo de cierta magnitud dejando el canal libre para otra conversación; pero la falta de sonido genera -tanto para el emisor como para el receptor- la sensación de que se interrumpió la comunicación. Para mantener la calidad de la comunicación se recurre a las técnicas de sidetone y confort-noise.
  - **Sidetone:** el emisor recibe en su oído una realimentación de lo que está diciendo.
  - **Confort-noise:** los codecs (hablaremos de ellos en la próxima edición) generan un ruido de fondo que brinda la sensación de una llamada activa.
- **Seguridad:** deben aplicarse mecanismos de seguridad que eviten posibles "espías" en la transmisión y que garanticen la integridad de la información.

En las siguientes ediciones, se analizarán estos puntos y sus posibles soluciones.

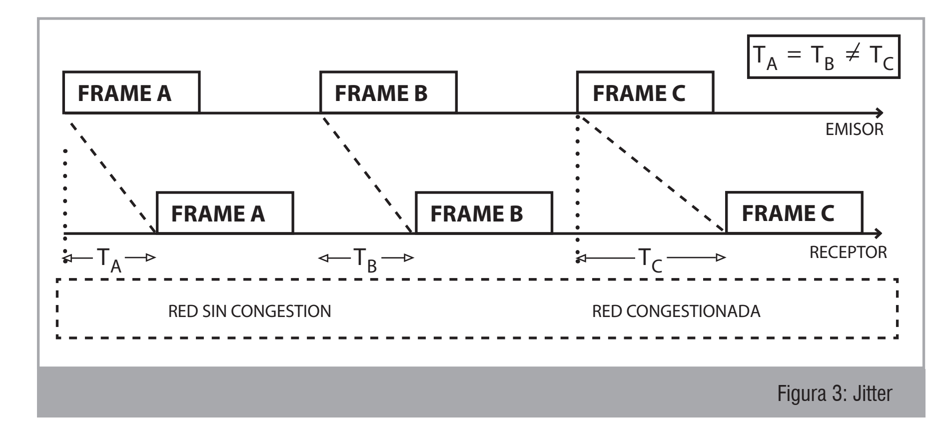


Figura 3: Jitter

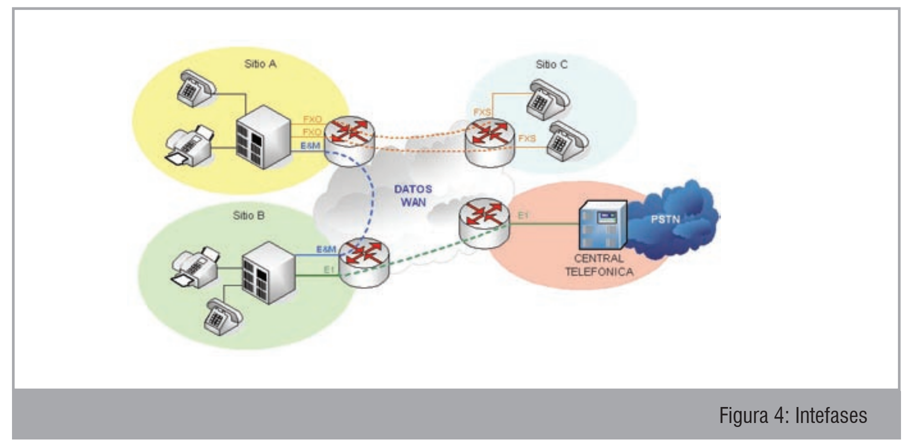


Figura 4: Intefases

Interfases

Las primeras aplicaciones de VoIP para telefonía privada consistían en vincular a través de la red de datos PABX, terminales telefónicos y faxes; hoy en día, conviven los dispositivos IP con los equipos telefónicos convencionales. Estos últimos no son capaces de transformar la señal analógica o digital PCM en apropiada para transmitirla como VoIP por lo que se necesitan interfases que permitan vincular un teléfono o fax analógicos, una PABX o la misma central telefónica del proveedor con el gateway que los vinculará a la red de datos. El tipo de interfase se diferencia de acuerdo a la señalización que se utilice; para el caso de las analógicas tenemos las siguientes:

- **FXS (Foreign eXchange Station):** se utiliza para conectar el router a un teléfono estándar, modem o fax; la misma provee tono, energía, detección de on-hook y off-hook y tensión para campanilla.
- **FXO (Foreign eXchange Office):** se utiliza para conectar el router a una central o PABX. Brinda señalización de loop (on-hook y off-hook) y necesita tono y energía para activarla.
- **E&M (Ear & Mouth o recEive & transMit):** se utiliza para señalización de troncal entre PABXs. La señalización E&M puede ser de tipo I, II, III, IV o V.

De la misma manera, existen interfases digitales que vinculan el gateway con una PABX mediante un acceso digital que generalmente son T1 o E1. Estas interfases pueden variar de acuerdo al tipo de señalización (ISDN y MFC-R2, son los más utilizados en nuestro país). La figura 4 muestra un ejemplo de los tipos mencionados.

Resumen

En este primer artículo, se plantearon los escenarios, los objetivos y las consideraciones para implementar VoIP. En la próxima edición, analizaremos los métodos de compresión y técnicas de QoS que aseguran un resultado exitoso en la transmisión de la voz.

Terminología

Esta serie aborda el tema de VoIP desde su origen y por lo tanto, pueden aparecer términos específicos de telefonía; para la lectura de éste y los próximos artículos, asumiremos que los mismos ya son conocidos por el lector. Si se desea información al respecto, se recomienda ingresar a la Web de la Comisión Nacional de Comunicaciones donde puede encontrarse documentación técnica y la normativa vigente en nuestro país (www.cnc.gov.ar).

Serie Voz sobre IP

Parte 1: Inicio, objetivos y requerimientos
Parte 2: Procesamiento de la voz y QoS
Parte 3: Protocolos
Parte 4: Telefonía IP

Autor: Juan Manuel Urti
Ing. en Telecomunicaciones (I.U.P.F.A.)

Traducción de Direcciones IP

Del Mundo Privado a Internet

FOTO: http://www.sxc.hu/ Andrew Brigmond



La traducción de Direcciones IP, denominada NAT –Network Address Translation-, es una manera efectiva de conservar el escaso espacio de direcciones Públicas ruteables a través de Internet. Además, es una manera útil de evitar que las redes Privadas de los clientes se solapen entre sí.

Introducción

El esquema de direccionamiento lógico más empleado hoy en las telecomunicaciones es el Internet Protocol Versión 4 – IPv4-. En este se define la longitud de las direcciones IP, las cuales constan de 32 bits, y a su vez se dividen en Clases del Tipo A, B, C, D y E. Las direcciones IP poseen una parte de red y una parte de host, la cual determina de qué Tipo son. A pesar de ello, y para no ingresar en detalles que hemos hablado en números anteriores, el espacio de direcciones disponibles para todo el mundo fue desde el inicio muy escaso.

De esas direcciones no todas son ruteadas en Internet y, según la RFC 1918 del IETF, se han reservado tres rangos a los fines de que las empresas empleen direccionamientos privados en sus redes LAN, evitando utilizar de una manera poco eficiente la mayoría de los espacios de redes públicas. (Estas direcciones reservadas podemos verlas en la figura 1).

Como se iban agotando rápidamente, primero se comenzó a usar la técnica de Máscaras de Longitud Variable –VLSM-, que permitió hacer un uso más eficiente de las redes más grandes y segmentarlas en subredes más pequeñas. A pesar de este pequeño remedio, el problema de fondo persistía porque no quedó más opción que trabajar en la Traducción de Direcciones a la hora de viajar en una red pública, como lo es hoy Internet.

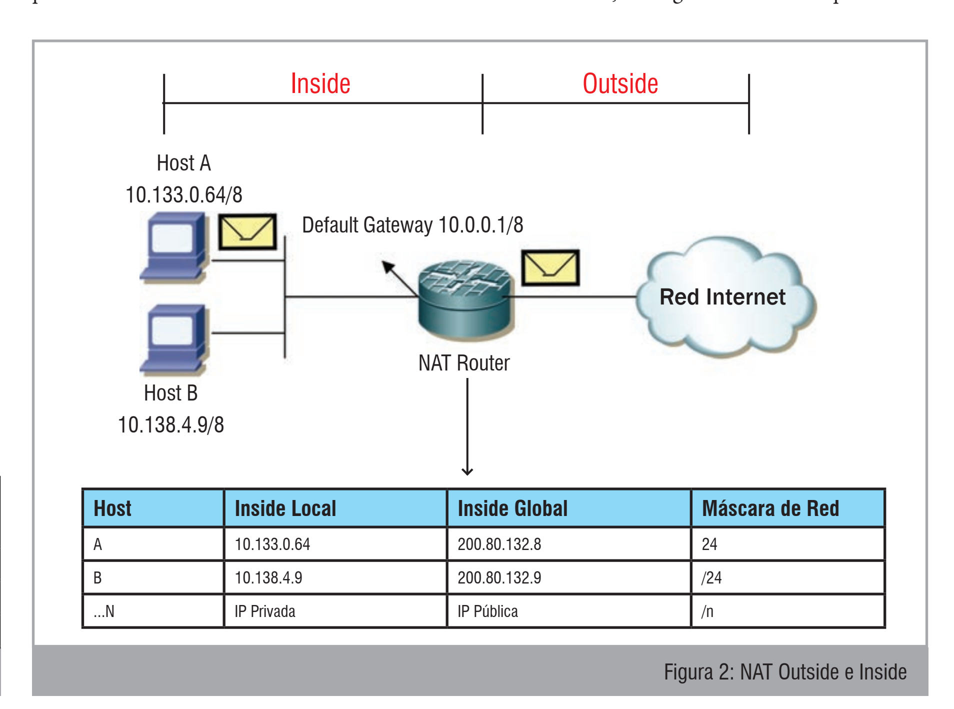
Clase	Desde	Hasta	Máscara de Red
A	10.0.0.0	10.255.255.255	/8
B	172.16.0.0	172.31.255.255	/12
C	192.168.0.0	192.168.255.255	/16

Figura 1: Rangos Privados de IPs

Network Address Translation (NAT)

Como no alcanzan las direcciones IP disponibles, para que cada PC de una red LAN posea una IP Pública –entiéndase como una dirección que se rutea por la Web-, fue necesario que las direcciones privadas que poseen configuradas las PC, o host de cada empresa, sean "traducidas" o "cambiadas" al momento de entrar al dominio público.

De esta manera los host poseen una dirección lógica visible desde la Web y otra dirección lógica dentro de la LAN. El equipo de nivel 3, ya sea un Router o un Firewall, es el encargado de realizar la traducción y recordar, por medio de una tabla, la asignación de cada par IP Pú-



Host	Inside Local	Inside Global	Máscara de Red
A	10.133.0.64	200.80.132.8	24
B	10.138.4.9	200.80.132.9	/24
...N	IP Privada	IP Pública	/n

Figura 2: NAT Outside e Inside

blica: IP Privada.

A raíz de lo mencionado, comentaremos cuáles son las terminologías que se agregan con esta aplicación:

- **Lado Inside:** Es la interfase del router o firewall que se conecta la red privada. En caso de que desee realizarse un NAT con direcciones del mismo tipo –ambas privadas por ejemplo- el segmento inside es el que posee las direcciones que nos interesa traducir.
- **Lado Outside:** Es el de la interfase pública o bien del segmento que es del dominio público.
- **Dirección Inside Local:** Es la dirección IP usada por el host, del lado privado, o sea del segmento Inside.
- **Dirección Inside Global:** Es la IP resultado luego de la traducción por una del dominio público.
- **Dirección Outside Local:** Es una IP Privada que se encuentra del lado público, que debe ser ruteable desde el lado inside.
- **Dirección Outside Global:** Es la IP pública de un host del lado habitualmente Internet. En una comunicación habitual, es la IP Pública Destino del paquete IP, que luego seguramente será traducida por otro equipo a una Outside Local.

Principio de Funcionamiento

Podemos tomar la figura 2 nuevamente como ejemplo, para explicar brevemente una situación normal de funcionamiento de una traducción de direcciones. Cuando un host envía un paquete a una dirección pública, como una página de Internet, utiliza como origen la Inside Local y destino la Outside Global (sería la



Protocolos soportados

NAT soporta la traslación de tráfico TCP y UDP que lleve las IPs destino y origen dentro del flujo de datos, soporta HTTP, TFTP, FTP, ICMP, IP Multicast y DNS entre otros. A pesar de ello no soporta la traslasión de Protocolos de ruteo, SNMP y DHCP.

Tráfico a NATear

El espacio de direcciones IP a ser pasible de translasión es definido por una lista de acceso. Estas pueden ser estándar o bien extendidas, soportando NAT ambos casos. Así mismo debe definirse por medio de alguna sentencia, que varían según el proveedor cuál es el pool o la IP pública a emplear como Inside Global.

outside local si hubiera un NAT bidireccinal). El paquete al llegar al dispositivo que realiza la traducción, cambiará la Inside Local por una Inside Global, a los fines de poder salir al dominio público. La dirección destino no sufrirá cambios, debido a que para el router esa IP no es conocida por algún mecanismo de ruteo. Aquí el paquete ya está en la red pública con Origen Inside Global y Destino Outside Global.

Cuando el paquete IP viaja en sentido contrario, el host destino genera el fragmento con Origen Outside Global y Destino Inside Global. Al llegar el router o firewall, este verifica la Tabla NAT y observa que hay una regla de sustitución de Ips, y por lo tanto ejecuta el cambio cambiando la Inside Global por la Inside Local.

Tipos de NAT
Clasificación y ejemplos

Básicamente existen tres tipos de NAT: NAT estático, NAT Dinámico y PAT –Port Address Translation-. Con estos podemos cubrir el espectro de posibilidades, en el cual traducimos una IP privada por una Pública en una relación 1:1; sino podemos traducir Privadas en m IPs Públicas, siendo m menos que n; o finalmente una IP Pública en N IPs Privadas, diferenciando cada host por medio de los ports TCP.

En la figura 3 podemos observar el primer caso que mencionamos, en el cual se produce una relación 1:1.

En este ejemplo, NAT Estático, se configura manualmente una traducción de direcciones lógicas en donde el router cambia la Inside Local por la Inside Global, que es con la que se presenta el host al dominio público.

Otra manera de traducir direcciones, pero empleando una sola dirección Inside Global es el PAT o también conocido por NAT Overloading. Aquí el router debe guardar en la tabla NAT información adicional, ya que de alguna manera debe recordar qué IP Local corresponde a una Global. La manera de realizar esto es que el router almacene información de nivel 4, por medio de puertos TCP/UDP. Así un host, y su correspondiente Inside Global, se identifica por el par IP Local:Port.

Tenga en cuenta que esa única IP puede ser reemplaza por un pool de IPs, digamos un bloque más pequeño que el espacio de direcciones IP de la LAN, permitiendo aún más traducciones. Este caso es conocido como NAT Dinámico.

Veamos la figura 4 para detallar lo mencionado. Cuando el Host A desea enviar una comunicación al Host con IP Outside Global 220.4.26.12, este envía un paquete al default gateway, ya que identifica que el equipo destino se encuentra en otra red IP. El router verifica la IP Inside Local y por medio de una lista de acceso entiende que esa IP es pasible de traslasión. El equipo toma una IP Inside Global del bloque dinámico para Natear –ese bloque puede ser de solo una IP, siendo PAT puramente- y cambia la Local por la Global, agregando un port TCP/UDP. De esta manera la IP Local queda conformada por el par IP Inside Global: Port.

Cabe mencionar que la relación IP: Port que se le asigna a un host del segmento Inside solo perdura mientras la sesión TCP esté activa, de modo que si ésta se cierra, se borra la relación de la Tabla NAT.

Por último debemos mencionar que el NAT no solo se usa para ingresar a la Web. Al haber tantas empresas que utilizan el esquema de direcciones privadas RFC 1918, sucede habitualmente que si dos empresas desean interconectarse por algún fin particular, es común que se solapen sus direcciones IP. Para evitar loops de ruteo, se estila colocar en la interconexión un router o firewall que permita traducir una de las redes LAN, entendiendo por esto un segmento IP no empleado por ambas entidades. ●

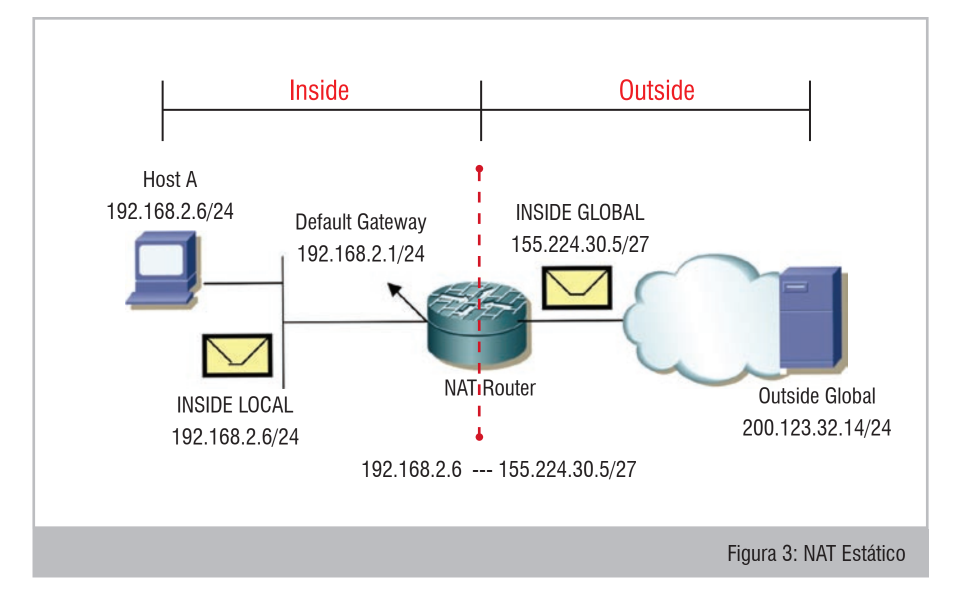
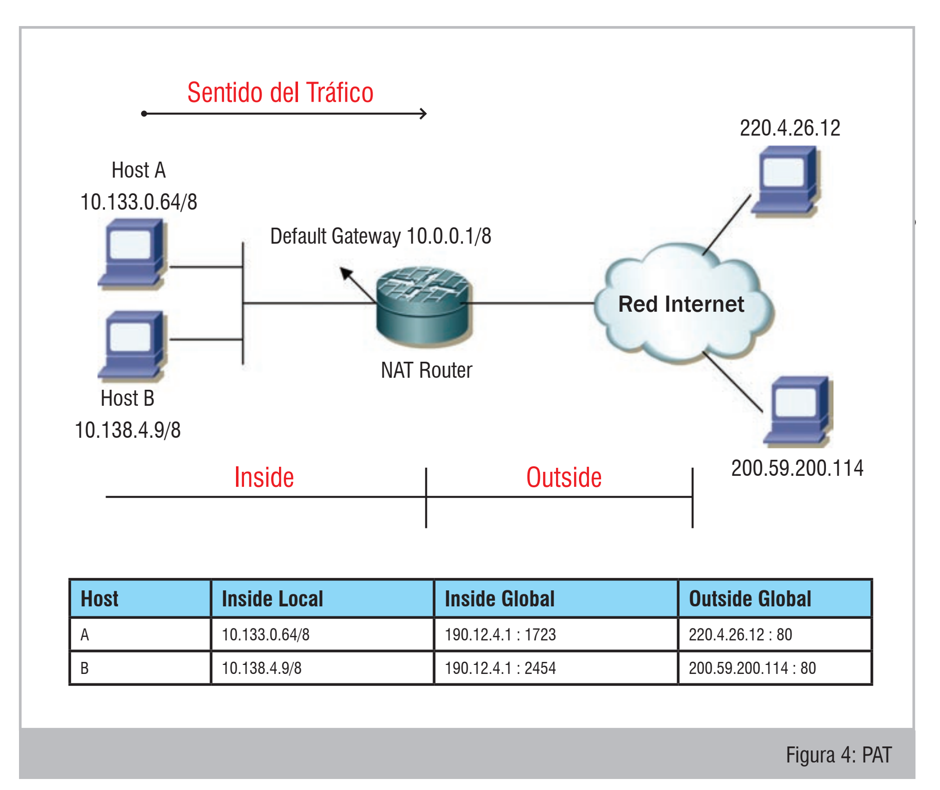


Figura 3: NAT Estático



Host	Inside Local	Inside Global	Outside Global
A	10.133.0.64/8	190.12.4.1 : 1723	220.4.26.12 : 80
B	10.138.4.9/8	190.12.4.1 : 2454	200.59.200.114 : 80

Figura 4: PAT

Autor: Fernando A. Luciague
Ingeniero Electrónico UBA)

FOTO: http://www.sxc.hu/ Josep Altarriba

RRPP Rapid Ring Protection Protocol

RRPP es el protocolo de la capa "nivel de enlace" utilizado en redes anillo Ethernet, de rápida convergencia y con un tiempo de convergencia independiente al número de nodos.

RRPP (*Rapid Ring Protection Protocol*) es un protocolo de la capa "nivel de enlace" utilizado en redes anillo Ethernet. Puede prevenir tormentas de broadcast causadas por loops cuando el anillo Ethernet está completo, puede rápidamente realizar el cambio al link de backup cuando el link en la red anillo Ethernet está desconectado y así recuperar los caminos de comunicaciones entre los nodos de la red.

Comparado con el protocolo STP *(Spanning Tree Protocol)*, el protocolo RRPP tiene las siguientes características:

- Rápida convergencia (menos de 50 ms).
- El tiempo de convergencia es independiente del número de nodos de la red.

Anillo RPR

RPR es un protocolo de la capa MAC, estandarizado por la IEEE 802.17 y la alianza RPR y es usado en la topología de anillo. El propósito del RPR es definir un loop cerrado, punto a punto y basado en la capa MAC en una topología de anillo. Para la capa física, RPR es un grupo de links punto a punto. Para la capa de enlace de datos, es una red de broadcast similar a Ethernet. RPR debe ser soportado por un hardware especial y un algoritmo complejo.

Anillo STP

El protocolo STP también es un estándar para la protección desarrollada por la IEEE. Es muy usado, pero en la práctica está limitado por la escala de la red y el tiempo de convergencia es afectada por la topología de la red. Cuando la red es de un diámetro grande, el tiempo de convergencia se ve afectado y la calidad de transmisión de datos puede ser afectada.

Para tener un tiempo de convergencia más corto y eliminar el impacto con una red de gran escala, Huawei-3Com desarrolló el protocolo RRPP.

Conceptos básicos

Dominio RRPP

El dominio RRPP está identificado por un ID. Un grupo de Switches que están configurados con el mismo ID de dominio, una VLAN de control y están interconectados constituyen un dominio RRPP. Un dominio RRPP contiene los siguientes elementos:

- **Anillo RRPP:** Físicamente corresponde a una topología Ethernet en anillo. Un dominio RRPP está compuesto por múltiples interconexiones de anillos RRPP, donde uno es el primario y el resto secundarios. Un dominio RRPP solo puede comprender un anillo RRPP. En el caso de un solo anillo, este podrá ser configurado como primario o secundario.
- **VLAN de control:** Cada dominio RRPP tiene dos VLANs de control llamados la VLAN de control mayor y sub-VLAN de control. Los paquetes de control del anillo primario son transmitidos en la VLAN mayor, mientras que los de los secundarios en la sub-VLAN.
- **Nodo maestro:** Es el nodo de control del anillo RRPP. Cada anillo RRPP debe tener solo un nodo maestro.
- **Nodo de tránsito:** Todos los nodos que no son el maestro son nodos de tránsito (los nodos de borde y los nodos de bordes auxiliares son nodos de tránsito especiales).
- **Nodos de borde:** Habrá dos intersecciones entre los anillos secundarios y el primario. El Switch en el punto de intersección es llamado nodo de borde y el Switch en el otro punto de intersección es llamado nodo de borde auxiliar. No existe ningún requerimiento en la configuración de los Switch de borde o en el auxiliar, mientras que los dos nodos se puedan diferenciar por su configuración.

Ejemplo de un Dominio RRPP

Como se muestra en la figura 1, el dominio 1 es RRPP y los Switches desde S1 a S6 pertenecen al dominio 1. La VLAN mayor y la sub-VLAN de control son VLAN3 y VLAN4 respectivamente. El dominio compromete dos anillos RRPP, anillo 1 y 2. El nodo maestro del primer anillo es S1 y el nodo maestro del anillo secundario es S6. S2, S3 y S4 son nodos de tránsito en el anillo primario, mientras que S5 es un nodo de tránsito del anillo secundario. Los nodos de borde y auxiliares del anillo secundario son S3 y S2.

Anillo RRPP

Cada anillo RRPP físicamente corresponde a una topología Ethernet anillo. El anillo RRPP es identificado por el ID. Cada anillo RRPP es parte del dominio RRPP donde se encuentra. Los anillos en el dominio RRPP están divididos entre el primario y secundario, que están diferenciados por sus niveles especificado durante la configuración. El anillo primario es configurado con el nivel 0 y el secundario con el nivel 1.

VLAN de control

Las VLANs de control en el dominio RRPP son utilizadas para transferir paquetes de RRPP. Cada dominio cuenta con dos VLANs de control, la mayor y otra secundaria o sub-VLAN. Donde los paquetes del anillo primario son transmitidos en la VLAN mayor y los paquetes de los anillos secundarios en la sub-VLAN.

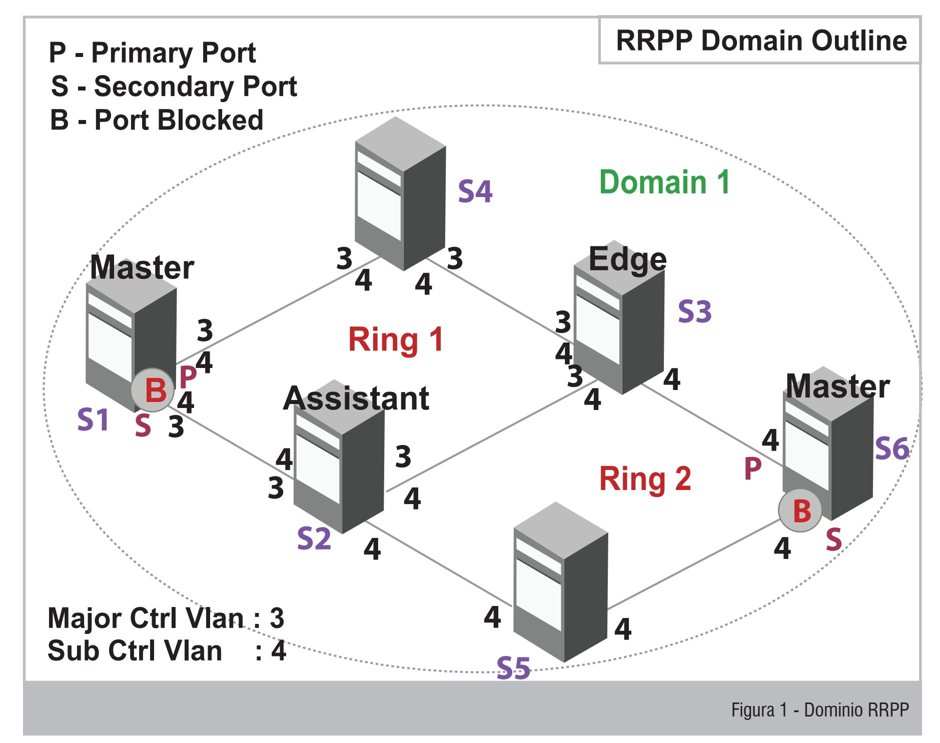


Figura 1 - Dominio RRPP

No se configura ip sobre estas VLANs. Los puertos en cada Switch para conectar el anillo Ethernet pertenecen a la VLAN de control y solo los puertos conectados al anillo Ethernet pueden ser sumados a la VLAN de control. Los puertos RRPP del anillo primario deben pertenecer a la VLAN mayor y al mismo tiempo a la sub-VLAN de control. Al contrario de las VLAN de control, las VLAN de datos son usadas para transmitir paquetes de datos. Puede comprometer puertos RRPP o no.

Nodo maestro

Cada Switch en el anillo Ethernet es un nodo, cada anillo RRPP debe tener un nodo maestro. Como se ve en la Figura 1, S1 es el nodo maestro del anillo primario y S6 es el nodo maestro del anillo secundario. El nodo maestro es el indicador del Polling. El nodo maestro envía un Hello periódicamente por su puerto primario si este no es recibido por el puerto secundario del nodo maestro, esto indica que hubo una falla en el anillo.

El nodo maestro tiene dos estados:

- Estado completado: Cuando todos los links del anillo están en estado UP y el nodo maestro puede recibir el hello. El nodo maestro refleja el estado del anillo RRPP. Una vez verificado que el anillo está completado, el nodo maestro va a bloquear el puerto secundario para prevenir un loop de broadcast de los paquetes de datos.
- Estado fallido: Cuando algunos de los links del anillo está en estado Down, esto indica que el nodo maestro está en estado fallido. En este caso el nodo maestro desbloqueará el puerto secundario para asegurar que la comunicación entre los nodos del anillo no sea interrumpida.

Nodo de tránsito

Todos los nodos que no son el maestro son nodos de tránsito.
Los nodos de tránsito tiene 3 estados:

- Estado Link-Up: En el Puerto primario y secundario están en estado UP.
- Estado Link-Down: Cuando el Puerto primario o secundario están en estado Down.
- Preforwarding state (temporalmente bloqueado): Cuando el Puerto primario o secundario está bloqueado.

Cuando un nodo de tránsito que está en estado Link-Up detecta un Link-down en el Puerto primario o secundario, éste va a pasar del estado Link-Up a Link-Down y va a notificar al nodo maestro del estado del link enviando un paquete de Link-Down.
El nodo de tránsito no cambia directamente del estado Link-Down al estado Link-Up. Cuando el link de un cierto puerto del nodo de tránsito pasa al estado Up y los dos puertos el primario y secundario están en estado Up, el nodo de tránsito pasa al estado *Preforwarding* y bloquea el puerto que se recuperó. Si se transita inmediatamente del estado Link-Up se puede producir un loop de broadcast de paquetes de datos. Es por esto que el nodo transita del estado Link-down al estado Preforwarding.

Nodo de borde

Como hay dos intersecciones entre los anillos primario y secundario, existen dos nodos de borde, uno llamado nodo de borde y el otro nodo de borde auxiliar. Existen 3 estados al igual que en los nodos de tránsito. La definición es la siguiente:

- Estado Link-Up
- Estado Link-Down
- Estado Preforwarding (temporalmente en estado bloqueado)

Base del RRPP

- Todos los nodos del dominio están configurados con el mismo RRPP ID y VLANs de control.
- El dominio tiene dos VLANs de control, una mayor y la otra sub-VLAN.
- Los paquetes del protocolo del anillo primario son transmitidos por la VLAN mayor, mientras los del anillo secundario por la sub-VLAN.
- El puerto RRPP en el anillo primario está sumado en la VLAN mayor y la sub-VLAN de control, mientras que el puerto RRPP en el anillo secundario está sumado a la sub-VLAN de control solamente.
- Los paquetes de protocolo del anillo secundario son procesados en el anillo primario como paquetes de datos y son bloqueados/desbloqueados en conjunto con los paquetes de datos.

El mecanismo de polling es un mecanismo utilizado por el nodo maestro del anillo RRPP para detector continuamente el estado del anillo. El nodo maestro envía un paquete de hello periódicamente desde el puerto primario. El paquete es transmitido en el anillo por los nodos de tránsito en turno. Si el paquete de hello enviado por el nodo maestro es recibido por el puerto secundario del nodo maestro, quiere decir que el link está completo. De otra manera, si el paquete hello no es recibido en un especificado tiempo, el nodo maestro considerara que hay una falta en el anillo. Si después que el nodo maestro haya cambiado a estado fallido recibe un paquete de hello, cambiará inmediatamente al estado completado, desbloqueando el puerto secundario, renovando el FDB y enviando por el puerto primario el paquete COMPLETE_FLUSH_FDB a los nodos de tránsito para que desbloqueen los puertos que se encuentran en estado Preforwarding y renovando la FDB.

Mecanismo de notificación del cambio de estado en el link

Compara con el mecanismo de Polling, el me

canismo de notificación de cambio de estado de link provee un mecanismo mas rápido para el manejo de los cambio de la topología de la red. El que inicia el mecanismo es el nodo de tránsito. El nodo de tránsito siempre monitorea el estado del link del puerto. Cuando hay un cambio de estado notificará al nodo maestro del cambio enviando un paquete de notificación para que decida como manejará el cambio. Cuando detecta que el puerto está en estado UP, el nodo de tránsito enviará un paquete de LINK-UP por el correspondiente puerto del anillo RRPP. Cuando detecte que el puerto está Down, enviará el paquete de LINK-DOWN.

Cuando existen múltiples anillos secundarios, se utiliza un protocolo del anillo secundario para la detección del estado del camino en el anillo primario, que es aplicado en redes donde existen múltiples anillos secundarios que intersectan el anillo primario. Los paquetes del anillo secundario son transmitidos entre los puertos de borde del nodo de borde y el nodo de borde auxiliar vía el camino suministrado por el anillo primario. Parece que el anillo primario es un nodo del anillo secundario. Cuando ocurre una falla en el link del anillo primario y el camino del paquete del protocolo del anillo secundario entre los nodos de borde y auxiliar está desconectado, el nodo maestro del anillo secundario no puede recibir el paquete hello enviado por sí mismo, entonces el tiempo de falla expira y el nodo maestro del anillo secundario transita al estado fallido y el puerto secundario será desbloqueado. Para redes comunes, esto es suficiente desde que no solo prevé loops de broadcast sino que existe un link de backup. Sin embargo, en las redes dual-homing mostrada en la figura 2, los anillos secundarios (anillo2 y anillo 3) están interconectados por los nodos de borde. Cuando el anillo1, el anillo primario, está en falta, los puertos secundarios del nodo maestro de cada anillo secundario son desbloqueados, y un loop de broadcast es inevitable entre los anillos secundarios (como se indica en la figura con las flechas).

Para remover tal efecto, el paquete del protocolo del anillo secundario de detección de estado del camino es introducido en el anillo primario. Es necesario que esté completado por los nodos de borde y los nodos de bordes auxiliares juntos. El propósito es bloquear el puerto de borde del nodo de borde antes que el puerto secundario del nodo maestro en el anillo secundario sea desbloqueado, así evitar loops de datos entre los anillos secundarios. El nodo de borde es el iniciador y el que toma la decisión del mecanismo y del monitoreo del estado del camino del nodo auxiliar de borde. Es responsable por la notificación oportuna del cambio de estado en el camino. La figura 3 muestra el efecto del mecanismo después que hubo una falla en el anillo primario.

Una restricción en la aplicación del mecanismo es que el puerto de borde del nodo de borde debe estar bloqueado antes que el puerto secundario del nodo maestro del anillo secundario.

Índices de performance

Todos los índices de performance son obtenidos de mediciones de práctica. Todas las pruebas son realizadas con seis nodos que corren el protocolo RRPP. Todos los nodos son Switches S3552P de Huawei-3Com, y todos los puertos son ópticos.

Los datos de performance son de convergencia de tráfico en L2. El máximo tráfico de convergencia de L2 es de 50 ms.

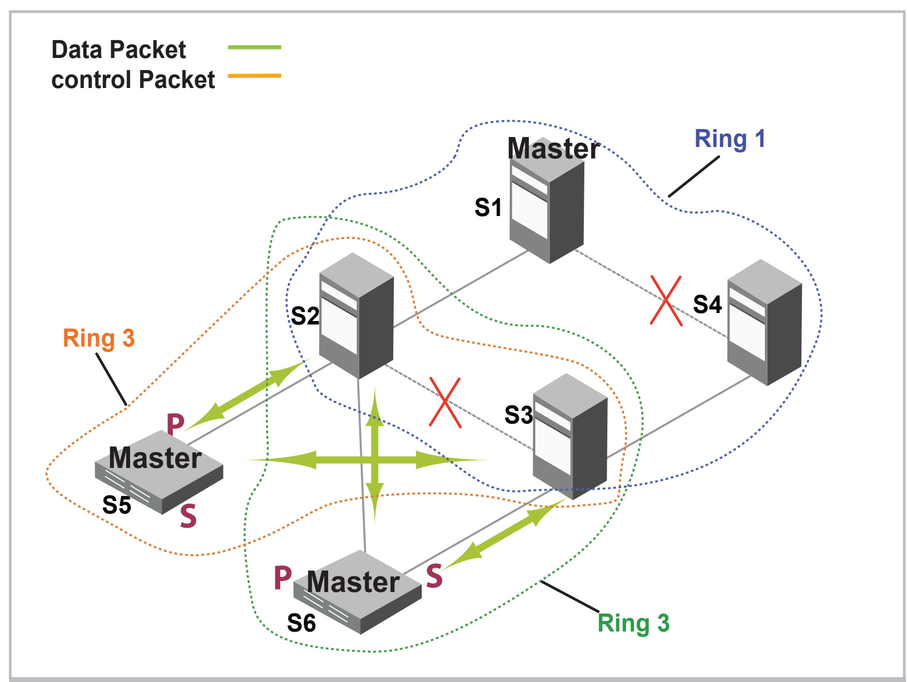


Figura 2: Loops de datos entre anillos secundarios en un dominio simple de una red multi-anillo sin mecanismo de detección de anillo secundario.

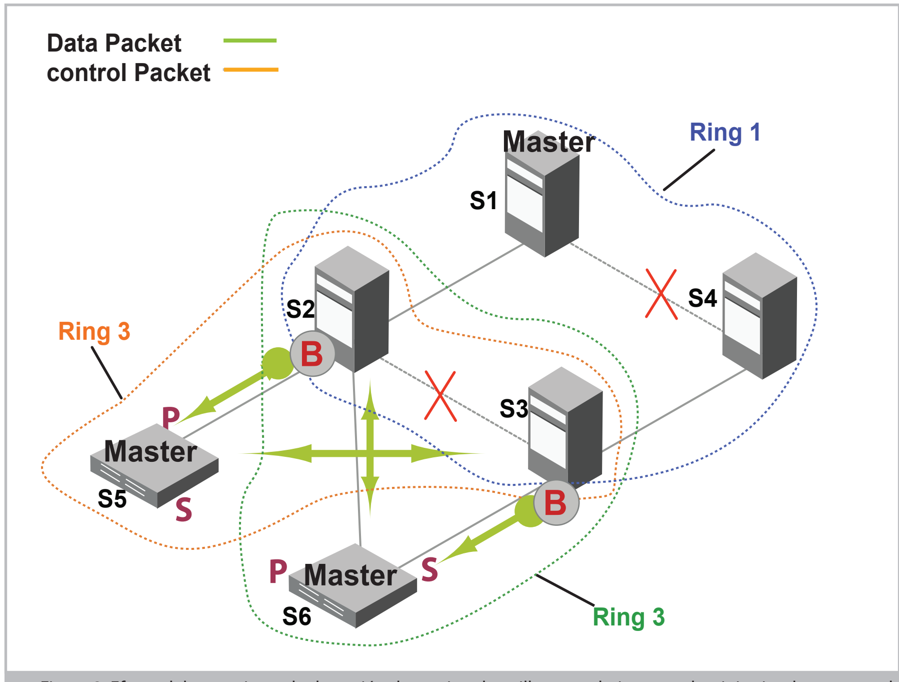
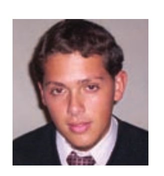


Figura 3: Efecto del mecanismo de detección de camino de anillo secundario en un dominio simple en una red multi-anillo.

Parte I de 2



Autor: Ariel Marcelo Liguori
Analista en Seguridad Informática

FOTO: http://www.sxc.hu/ Michal Zacharzewski



Siguiendo el camino con MPLS

El crecimiento exponencial de la demanda de ancho de banda y la creciente necesidad de una solución a la problemática que implica el no poder proveerlo encuentra su respuesta en un modelo prometedor, MPLS.

El surgimiento de nuevos servicios tales como VoD (Video on demand), VoIP, Videoconferencia, etc. ha desatado una continua demanda de ancho de banda y calidad por parte de los usuarios finales. Tecnologías como ATM e IP, deben ceder su lugar a un método integrador que provea la solución adecuada para tales necesidades, aquí se halla el surgimiento de MPLS (Multiprotocol Label Switching).

En 1997 el IETF (Internet Engineering Task Force) comienza el proyecto MPLS, el cual culmina en 1998, año en el que se define el estándar MPLS en el RFC3031. Detrás de MPLS se esconde una tecnología de conmutación de paquetes con soporte multiprotocolo que utiliza métodos de enrutamiento basado en la asignación de flujos dentro un sistema autónomo (AS). Una característica útil que brinda MPLS es la posibilidad de diferenciar y manejar fácilmente estos flujos, logrando de este modo no congestionar la red (estableciendo, por ejemplo, una ruta paralela y desviando el tráfico en momentos de gran consumo).

Las ventajas principales que ofrece MPLS son:

- Clara independencia entre L2 y L3.
- Fácil integración en redes IP, ATM y Frame Relay.
- Traducción de direccionamiento IP en etiquetas de longitud fija.
- Flexibilidad en el enrutamiento de la red.
- Soporta QoS y CoS.
- Gran escalabilidad de la red.
- Ingeniería de Tráfico y DiffServ.
- Ahorro de costos.

Componentes de una red MPLS

Una red MPLS está constituida esencialmente por routers MPLS llamados LSR (Label Switching Router), ubicados como equipos core dentro del backbone; y por otros routers MPLS llamados LER (Label Edge Router), los cuales establecen la conexión con otras redes. Los LSR son los encargados del establecimiento de los circuitos extremo-extremo dentro de la red, denominados LSPs (Label Switched Paths), y de la redirección del tráfico sobre estos caminos. Los LER se diferencian en dos tipos, los nodos de entrada y los nodos de salida.

El LER de entrada se encarga de examinar la información entrante y de acuerdo a una base de datos en la cual se establece la QoS (Calidad de Servicio, Quality of Service) requerida asigna una etiqueta (label) al paquete; en los nodos de salida se produce el camino inverso, los LER son los encargados de remover las etiquetas para restaurar el paquete. El LER brinda el soporte multiprotocolo.

Etiqueta MPLS

La etiqueta MPLS (ver figura 1) posee una longitud de 32 bits, los primeros 20 corresponden a la etiqueta; los siguientes 3 son considerados de uso experimental, anteriormente eran llamados CoS (Clase de Servicio, Class of Service) ya que determinaban la QoS del paquete y gracias a este campo era posible diferenciar distintos tipos de tráficos y mejorar el rendimiento de alguno de ellos en particular. Otro bit es el de STACK, el cual permite apilar diversas etiquetas en orden jerárquico, el valor del stack es cero cuando aún hay más etiquetas en el paquete y cuando el stack vale uno significa que esa es la última etiqueta del paquete. Los últimos 8 bits corresponden al tiempo de vida del paquete o TTL (Tiempo de vida, del inglés Time To Live).

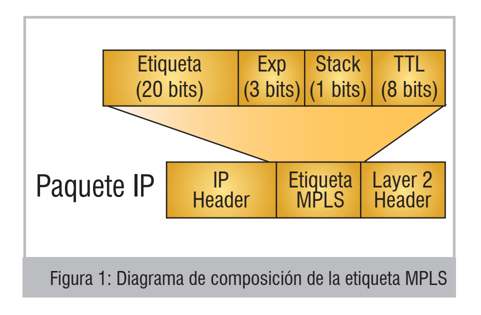


Figura 1: Diagrama de composición de la etiqueta MPLS

Funcionamiento de una red MPLS

Como ya se ha enunciado el LER es el que establece la conexión con la red externa, recibiendo un paquete y asignándole luego una etiqueta. Cuando un paquete ingresa a la red se le asigna un determinado FEC (Clase Equivalente de Direccionamiento, del inglés Forwarding Equivalent Class). Un FEC es la representación de un conjunto de paquetes que comparten idénticas características de transporte, de este modo todos los paquetes pertenecientes a un mismo FEC seguirán los mismos LSP para alcanzar el destino. El LER en un esquema simple asigna una etiqueta y un FEC al paquete utilizando tablas preprogramadas (ver figura 2), luego del "etiquetado" el paquete comienza su viaje a través de la red MPLS, en esta trayectoria se encuentra con un LSR el cual examina la etiqueta y la compara con una tabla propia llamada "Base de información de Etiquetas" (LIB, por sus siglas en inglés). Tras este proceso se determina cuál será el siguiente "salto" de ese paquete y a la vez se cambia la etiqueta por una nueva, que será analizada por el próximo LSR, en el que se repetirá el proceso hasta que finalmente se llegue al nodo de salida que eliminará la etiqueta y la entregará al destino.

Armando el camino: Establecimiento de los LSPs

Básicamente se pueden distinguir dos mecanismos para crear un LSP dentro de una red MPLS:

Método de encaminamiento salto a salto (hop-by-hop): En éste cada LSR selecciona el próximo salto para un determinado FEC, para esto utiliza alguno de los protocolos de enrutamiento soportados por el dispositivo (OSPF, ATM PNNI, etc.).

Método de encaminamiento explícito: En este caso el LER de entrada es quien determina la secuencia de saltos a seguir hasta llegar al destino. Suele haber casos en que la ruta no está completamente especificada y también se pueden hallar identificadores de Sistemas Autónomos en las mismas.

El protocolo MPLS permite el establecimiento de LSPs primarios y secundarios, la lógica para la designación de estos LSPs se realiza en base a algoritmos de encaminamiento con QoS que se encargan de localizar los recorridos óptimos teniendo en cuenta la QoS que se requiera y el uso de los recursos de red. Desde este punto y en adelante la gestión de los recursos consiste en ajustar los LSP establecidos de manera de satisfacer las demandas que se encuentren en la red. Para lograr una adaptación "on demand" al tráfico real de la red la implementación de MPLS va en conjunto a sistemas de Ingeniería de Tráfico o TE (Traffic Engineering), los cuales están constantemente chequeando la integridad del BackBone. Los sistemas de gestión están relacionados con el manejo de los LSP, es por ello que generalmente estos sistemas son los encargados de la detección de alarmas y de la activación de los LSP secundarios, para ello el sistema debe tener suficiente información sobre el estado real de la red para distribuir los LSP según sean las demandas reales de trafico. Si bien esto responde automáticamente a los fallos de la red y crea un enlace secundario para que el usuario final no perciba el problema hay distintas dificultades que se pueden atravesar luego del establecimiento de un LSP de respaldo. Los casos de error más comunes son:

- Al cabo de un tiempo determinado la demanda de tráfico supera la reserva inicial del LSP y se produce un rechazo de tráfico.
- El ancho de Banda asignado a un LSP es mucho mayor que el tráfico demandado, lo cual resulta en un desperdicio de recursos.

Diversas técnicas están orientadas a evitar este tipo de incidentes en la red, basándose siempre en un sistema de gestión que, según sea la situación, actúe de manera eficiente asignando, en base a las demandas reales y en tiempo real, los LSP que sean necesarios. Al hablar de estos sistemas y mecanismos hacemos referencia directa a un "entorno global de ingeniería de tráfico". Ahondando en este tema descubriremos que varias soluciones tratan de satisfacer los requisitos pero aún no se define cuál es mejor de ellas, estamos haciendo referencia a sistemas centralizados o sistemas distribuidos de ingeniería de tráfico. En grandes redes se dificulta poseer todos los datos de monitorización de forma centralizada y esto puede llevar a no poder calcular la distribución óptima de los recursos a tiempo, es decir antes de que el estado ya haya cambiado. Una tendencia que apunta a la optimización de estos inconvenientes es la basada en algoritmos distribuidos, en los cuales cada uno de ellos posee la información de su "zona" permanentemente actualizada, no obstante una desventaja que se encuentra en ellos es que no poseen una visión global de la red.

Algo que no debe escapar de nuestro análisis

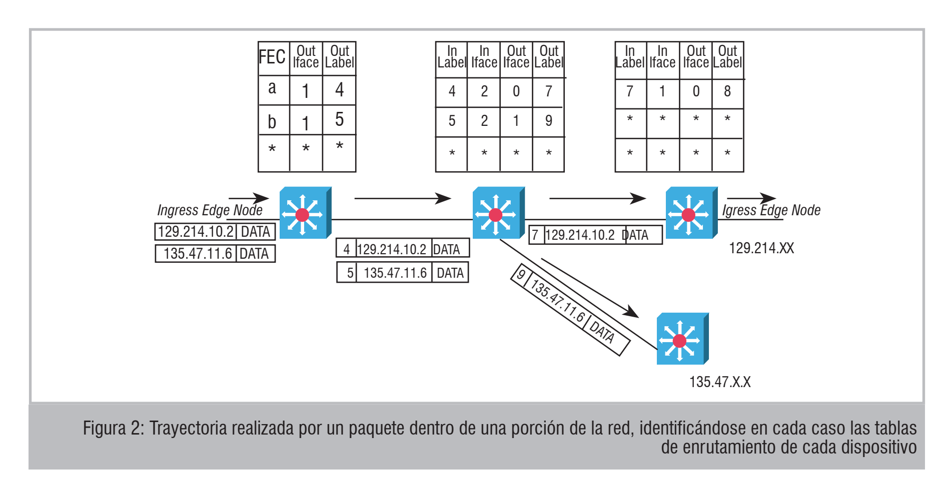


Figura 2: Trayectoria realizada por un paquete dentro de una porción de la red, identificándose en cada caso las tablas de enrutamiento de cada dispositivo

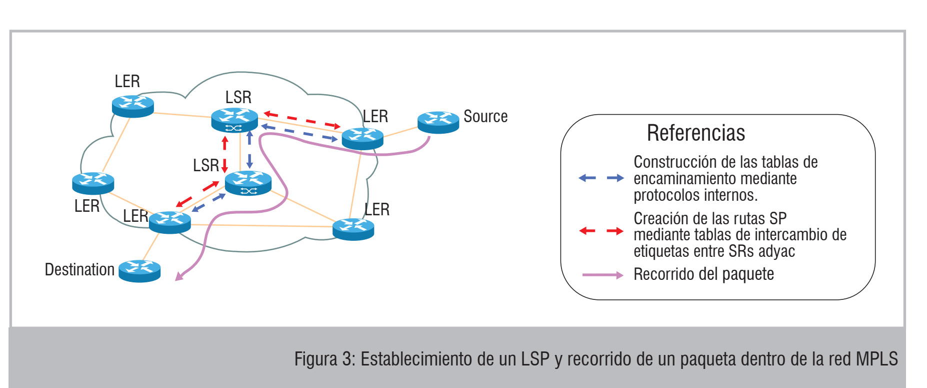


Figura 3: Establecimiento de un LSP y recorrido de un paqueta dentro de la red MPLS

es cómo se distribuyen las etiquetas.
Según se decida, los LSR pueden intercambiar esta información mediante diversos protocolos de distribución de etiquetas. El protocolo de distribución es el conjunto de procedimientos empleados por un LSR para comunicarle a otro la relación etiqueta – FEC que se ha establecido. Dependiendo de cómo se establezcan los LSP se pueden presentar distintos métodos de distribución. Si se utiliza la aproximación salto-a-salto (hop by hop) para el establecimiento de los LSP el IETF ha designado el protocolo LDP (Protocolo de distribución de etiquetas, del inglés Label Distribution Protocol), no obstante esto no es obligatorio y en consecuencia se pueden usar otros como ser RSVP, etc. Si la estrategia utilizada es “Downstream unsolicited”, en la cual el LER de salida distribuye las etiquetas a usarse para alcanzar un determinado destino (nótese que envía las tablas sin una solicitud previa), debe usarse LDP. Cuando se está trabajando con “Downstream on demand” (el LSR solicita las tablas al LER, el cual sólo se las enviará tras recibir dicha solicitud) iniciado desde el LER de entrada y no se desea seguir un camino calculado step-by-step sino que queremos utilizar rutas explicitas se utilizará CR-LDP y RSVP / RSVP-TE respectivamente.
Introduzcámonos ahora en cada uno de estos diversos protocolos para entender desde su interior cómo se realiza cada asignación.

• **El protocolo LDP:** El intercambio de mensajes entre LSRs se realiza mediante el envío de PDUs (Protocol Data Unit) de LDP, el mismo está basado en el establecimiento de sesiones LDP sobre conexiones TCP. Una característica a remarcar es que cada LDP PDU puede transportar más de un mensaje LDP en donde cada uno de éstos puede ser autónomo de otro.

• **El protocolo CR-LDP (Constraint-Based Routing Label Distribution Protocol):** Es una extensión del LDP y, como su nombre lo indica, se basa en el cálculo de trayectos sujetos a restricciones, las cuales serán: demanda de QoS, demora o delay, variación del delay (comúnmente conocido con el nombre de jitter), tasa de pérdidas, etc. El IETF lo ha definido específicamente para soportar establecimiento y mantenimiento de LSP encaminados de forma explícita.

Las limitaciones de este protocolo están definidas en el RFC3213 y son las siguientes:

- Solo soporta LSP’s punto a punto.
- Solo soporta el establecimiento unidireccional de LSP’s.
- Solo soporta una única etiqueta por LSP.

• **El protocolo RSVP-TE (Extensiones de RSVP para túneles LSP):** El protocolo RSVP (Resource Reservation Protocol) es utilizado para la reserva de recursos para una sesión en la red, su objetivo es asignar, en base a la demanda, la QoS requerida.
La implementación de este protocolo sobre redes MPLS requiere una extensión sobre los objetos del protocolo inicial, dichos cambios están definidos en el RFC3209 y dan surgimiento a RSVP-TE. Se puede utilizar RSVP-TE para establecer LSPs en el modelo downstream on demand.
Un requisito adicional para este protocolo es que el dominio MPLS debe soportar el método de encaminamiento explícito para gestionar de manera eficiente el tráfico, esto encuentra solución en el agregado de un objeto (el valor EXPLICIT_ROUTE) a los mensajes del path.

Una de las mayores ventajas de la utilización de RSVP-TE para el establecimiento de túneles es que permite realizar la asignación de recursos a través del camino, no obstante no se requiere la reserva de recursos en el momento del establecimiento del LSP.

• **Aplicaciones de MPLS:** La tecnología MPLS ha impactado en el mercado dando notables mejoras y aplicaciones, entre las cuales se destacan:
• *Ingeniería de Tráfico (TE):* La TE hace referencia a la capacidad de seleccionar los caminos que seguirá el flujo de datos a través de la red balanceando la carga de la misma con el fin de evitar que alguno de los recursos se encuentre infrautilizado o sobrecargado, las consideraciones sobre su uso se encuentran definidas en el RFC2702.

Las ventajas que agrega MPLS sobre este entorno son básicamente:

1) Mediante el establecimiento de rutas explícitas se posee el camino exacto para determinar un LSP.
2) Con la utilización del enrutamiento basado en restricciones se puede determinar las rutas para cada servicio en particular.
3) Se pueden obtener estadísticas de tráfico de los distintos LSP.

• *Servicios con CoS:* El RFC3270 define el manejo de servicios diferenciados mediante la utilización de una red MPLS, una gran cualidad de este protocolo es que soporta diferente clases de servicio por cada LSP y en particular puede soportar varias clases sobre un mismo LSP. MPLS se adapta a este servicio ya que cuenta con un campo dentro de su etiqueta (el campo Exp) para propagar la clase de servicio dentro del LSP, además la integración de MPLS con DiffServ agrega las facilidades de Queue y de Drop Priority (Prioridad de Descarte).

• *MPLS VPN:* Las VPN MPLS están basadas en el establecimiento de túneles LSP. Al aplicar etiquetas a los datos que ingresan en la VPN un LSR podrá separar el flujo de ésta de los demás flujos del BackBone del proveedor de servicios. El RFC2547 define la implementación de este servicio. Básicamente las ventajas que aporta MPLS a las VPN son:

1) Aplicación de TE.
2) QoS sobre el flujo de datos de la VPN (solo con reservar recursos para el túnel LSP).
3) Escalabilidad.
4) Modelo Acoplado de MPLS VPNs.

En la segunda parte de esta nota veremos cómo ha evolucionado la tecnología MPLS, su adaptación a redes ópticas y el nivel de integración conseguido en la definición de un nuevo estándar que tiene como único fin la uniformización de los esquemas de red y su intercomunicación, claramente haremos referencia a GMPLS y su estructura. •

Referencias y Links de Interés

- IP/MPLS Forum: http://www.ipmplsforum.org
- RFC: http://www.rfc-editor.org/
- IETF: http://www.ietf.org/

CERTIFICACIONES



Como venimos haciendo hace ya varios issues, en este caso elegimos la reconocida certificación del LPI, les contamos un poco acerca de esta institución y les acercamos algunas preguntas de sus exámenes.

A medida que el open source se hace más popular crece con el la cantidad de profesionales que se vuelcan a esta tecnología y que deciden corroborar los conocimientos adquiridos mediante las certificaciones.
Una de las de mayor renombre en la industria es la LPI. **El Linux Professional Institute** fue originalmente conformado en Octubre de 1999 como una asociación canadiense sin fines de lucro. Dos años después ya estaba ganando el Linux Journal's Editor's Choice Award por realizar una investigación exhaustiva antes de comenzar sus exámenes de certificación, con el fin de determinar qué habilidades realmente utilizan los profesionales de GNU/Linux en sus trabajos.
En la actualidad la certificación LPI está disponible en varios idiomas y en cientos de lugares en el mundo y con el apoyo de empleados, vendors y entrenadores.

Existen tres niveles en la certificación:

LPIC1: Consta de los exámenes 101 y 102 y es de nivel básico.

LPIC2: Consta de los exámenes 201 y 202 y es un nivel intermedio.

LPIC3: Es el más nuevo (tiene un año de vigencia) y representa la culminación de la certificación LPI. Consta del examen 301 y 302.

Datos

- El costo de cada uno de los exámenes es alrededor de $150 dólares, pero pueden variar según la región.
- Los exámenes se pueden tomar a través de las páginas de Pearson VUE y Prometric.
- Los exámenes están disponibles en inglés, chino, francés, portugués y castellano.
- Para aprobar los exámenes se debe lograr un puntaje mínimo de 500 en el 101 y 102 y de 530 en el 201 y 202.
- Una vez obtenida la certificación, para mantenerla activa se debe rendir un examen de recertificación a los cinco años.
- Libro recomendado: LPI Linux Certification in a Nutshell.

PRUEBE SU CONOCIMIENTO

Examen 101

1 Mónica consulta el *archive /etc/passwd* esperando encintrar passwords encriptados de todos los usuarios de su sistema. Esto es lo que ve:

jdoe:x:500:500::/home/jdoe:/bin/bash
bsmith:x:501:501::/home/bsmith:/bin/tcsh

¿Cuál de las siguientes es verdadera? Seleccione una.

a) Las cuentas *jdoe* y *bsmith* no tienen password.
b) Las cuentas *jdoe* y *bsmith* están deshabilitadas.
c) Los passwords están en */etc/passwd-*
d) Los passwords están en */etc/shadow*
e) Los passwords están en */etc/shadow-*

Respuesta correcta: d) la x a continuación de os nombres de usuarios denota que los passwords fueron colocados en el /etc/shadow.

2 ¿Qué contiene el directorio /sbin? Seleccione la mejor respuesta.

a) Los comandos necesarios en caso de una emergencia del sistema y que son de interés para todos los usuarios del sistema.
b) Los comandos de interés para todos los usuarios del sistema.
c) Los comandos necesarios en caso de una emergencia del sistema y que son de interés solo para el administrador.
d) La librería de interés solo para el administrador.

Respuesta correcta: c) Mientras que las respuestas b) y d) son técnicamente correctas, la c) es la que mejor describe a /sbin.

Examen 102

1 *¿Cuál de los siguientes representa una secuencia válida de comandos para compilar e instalar un nuevo kernel?*
Elija una.

a) make modules_install; make modules; make bzImage, make clean; make dep
b) make dep; make clean; make bzImage; make config; make modules; make modules_install
c) make config; make dep; make clean; make bzImage; make modules; make modules_install
d) make config; make bzImage; make dep; make clean; make modules; make modules_install
e) make dep; make clean; make bzImage; make modules; make modules_install; make config

Respuesta correcta: c) La respuesta a) es incorrecta porque instala los módulos antes de compilarlos. La b) y la e) también son incorrectas porque crea el kernel luego de configurarlo. La d9 va hacia atrás.

2 *Cuántos host pueden existir en una subset con una máscara 255.255.255.128? Les dasmos las opciones y se debe seleccione solo una como correcta.*

a) 512
b) 256
c) 128
d) 127
e) 126

Respuesta correcta: e) Al 128 resultante de realizar 27 se le resta la dirección de red y de broadcast, lo que deja 126 direcciones para hosts.

Examen 201

1 No logra que un servidor Samba funciones. Chequeó en el archivo /etc/samba/smb.conf y notó que las siguientes líneas no fueron comentadas:
wins support = yes
wins Server = 192.168.2.33

De estas líneas, puede resolver que el problema es que:

a) el servidor Samba está intentando acceder a través de un servidor WINS que no funciona.
b) El servidor WINS está utilizando una dirección privada de IP.
c) La entrada wins support deberá leer wins support = 1.
d) El servidor Samba está configurado para ser tanto un cliente WINS como un servidor WINS.

Respuesta correcta: d) El servidor Samba no puede ser configurado para ser un cliente WINS y un servidor al mismo tiempo.

2 Considere el siguiente archivo */etc/raidtab:*

raiddev /dev/md0	*raid-level 1*
nr-raid-disk 2	*chunk-size 64k*
persistent-superblock 1	*nr-spare-disks 0*
device /dev/hda2	*raid-disk 0*
device /dev/hdc2	*raid-disk 1*

¿Cual de los siguientes comandos en necesario para activar esta configuración?

a) mdadm /etc/md0
b) mkraid /etc/md0
c) mdadm /dev/md0
d) mkraid /dev/md0

Respuesta correcta: d) El comando mkraid es utilizado para procesar instrucciones en archivos fuera del directorio /etc, en este caso /etc/md0.

Examen 202

1 Quiere agregar una segunda dirección de IP a su tercera tarjeta Ethernet. ¿Cuál de los siguientes comandos realiza esta acción?

a) ifconfig eth3:2 202.168.85.3 netmask 255.255.255.0
b) ifconfig eth0:3 202.168.85.3 netmask 255.255.255.0
c) ifconfig eth1 –a 2 202.168.85.3 netmask 255.255.255.0
d) ifconfig eth2:1 202.168.85.3 netmask 255.255.255.0

Respuesta correcta: d) Cuando utilice el comando ifconfig para especificar una segunda dirección de IP para un NIC, debe hacerlo de esa forma.

2 Sospecha que varios routers en una conexión WAN particular son muy lentos. ¿Cuál de los siguientes comandos le permite hacer que un traceroute espere 20 segundos para responder a un paquete?

a) traceroute -w 20 router23.company.com
b) traceroute -c 20 router23.company.com
c) traceroute -i 20 router23.company.com
d) traceroute -t 20 router23.company.com

Respuesta correcta: a) la opción -w en un traceroute le permite especificar el período de espera. Traceroute esperará por default 5 segundos y luego se moverá al siguiente hop.

Autor: Federico Nan
Nantec Soluciones

¿Tu Linux está seguro?

Introducción al Hardening en sistemas GNU/Linux.

La seguridad es una sensación. Nunca ningún sistema va a estar seguro 100 por ciento; esto es algo que todos los que trabajamos en sistemas lo tenemos claro. Ahora bien, se pueden hacer algunas cosas para que este nivel no sea tan bajo y, nuestros sistemas, no estén abiertos a los famosos "Script Kiddies".

Hoy es muy común escuchar términos como "defacing", "sql injection", "buffer overflow", entre otros.

Es bien sabido que estas técnicas no son ninguna novedad y tienen sus años, pero muchos informáticos pasan por alto este tipo de información y configuran su sistema de manera "rápida" y "robusta". Se olvidan, a veces, de un factor fundamental: la seguridad.

Estamos muy acostumbrados a instalar un sistema operativo con la finalidad de que "salga andando" lo más pronto posible y con la menor cantidad de complicaciones (si anda no lo toques!).

Muchos siguen un "how to" que encontraron por Internet o copian la configuración que les pasó un "amigo" que sabe más que ellos. Es muy común que la velocidad de las empresas haga que los encargados de sistemas no reparen en este pequeño "detalle" de la seguridad.

GNU/Linux tiene fama de ser un sistema operativo seguro. Yo creo que el único sistema operativo seguro es el que está apagado. Es cierto que un Volvo C70 es un auto seguro, pero a 180 Km/h y sin cinturón de seguridad nuestras posibilidades de sobrevivir bajan. Lo mismo pasa con GNU/Linux. Su arquitectura es segura, pero hay que estar atentos a lo que nosotros hacemos con todo eso.

Las herramientas que les quiero presentar hacen que GNU/Linux sea un poco más seguro. En esta entrega, son solo dos, pero creo que, para empezar, alcanza y sobra.

Hay varios proyectos que se ocupan de la seguridad en el kernel y los programas.

Las distribuciones actualizan sus repositorios con una velocidad casi perfecta, para que los usuarios tengan sus nuevas versiones con parches listos para descargar.

El grupo de desarrollo del kernel hace lo propio con sus versiones, manteniéndolas lo más seguras posibles.

Podemos agregarle algunos condimentos extras a todo esto.

Conclusión

Mi idea no fue la de mostrar cómo usar las herramientas, sino la de mostrarles estos programas que pueden ayudarnos a defender nuestros sitios y sistemas de posibles ataques. Hay mucho por investigar en cada uno. Les dejo algunas páginas Webs que pueden ser interesantes:

http://www.modsecurity.org
http://www.grsecurity.net
http://www.nsa.gov/selinux/

Para los que quieran probar algunos exploits....
http://www.milw0rm.com/

HERRAMIENTAS DE SEGURIDAD

Grsecurity

Esta herramienta se puede aplicar al Kernel de Linux y es una de mis preferidas. La instalación no es difícil para un administrador con conocimientos medios. Solo hay que bajar el parche de la página oficial y recompilar el kernel (preferentemente Vanilla). Al momento de la configuración del Kernel, una nueva solapa de seguridad nos mostrará una cantidad de opciones que harán de nuestro sistema un lugar más seguro. Podemos configurar:

- **PAX** (una buena solución para limitar los buffer overflows).
- **RBAC** (Role-Based Access Control) donde podremos configurar policies para nuestros usuarios de sistema.
- Un mejorado chroot (enjaulado) para procesos.
- Muchas herramientas extras de audición y logging del sistema.

Para los que todavía no se animan a configurar por partes, Grsecurity tiene tres niveles por default que nos pueden ayudar a empezar (Seguridad Baja-Media-Alta).

Una vez configurado, solo resta compilar y reiniciar con el nuevo Kernel, para ir notando algunos cambios.

Sin administración responsable, este tipo de herramientas no sirven, e incluso podrían terminar molestando más que ayudando.

Es importante acompañar esta instalación con alguna guía básica de seguridad de cada distribución en particular; por ejemplo la de Debian es: http://www.debian.org/doc/manuals/securing-debian-howto/

Mod Security (Apache)

Otro método que vuelve locos a los administradores de sitios Webs son las técnicas de Blind SQL Injection, XSS y todo tipo de Defacing que hace que nuestras páginas estén un poquito inseguras. Como administradores podemos frenar los ataques a los servidores Web.

En el caso de Apache, el Mod Security nos permite crear un "firewall" entre el cliente y nuestro sitio. Este módulo se encarga de leer todos los request HTTP en tiempo real. Cuenta con la posibilidad de loguear cualquier evento y también ejecutar acciones (reglas) para la defensa de los sitios. Contiene varias reglas básicas de filtrado y un buen lenguaje para programar las propias. A diferencia de un IDS (como el Snort), este programa puede trabajar con páginas encriptadas por HTTPS. La página oficial es: http://www.modsecurity.org/.

Instalarlo en Debian, lleva solo unos minutos.



Con el lanzamiento de la versión 8.04, del sistema operativo de código abierto más popular y exitoso de los últimos tiempos, Ubuntu vuelve a estar en boca de todos.
Los desarrolladores de Ubuntu han logrado combinar en un único sistema los beneficios y posibilidades del Open Source con una interfaz amigable digna de los mejores softwares de código cerrado.
La industria por su parte comienza a mirar a Ubuntu con otros ojos, y cada vez más fabricantes apuestan por ofrecer computadoras con este software de código abierto precargado, mientras que el mercado de los servidores, que siempre fue más proclive a las soluciones basadas en Linux, lo ha recibido con los brazos abiertos. Por todas estas razones, puede resultar una buena opción el capacitarse en un sistema operativo que por ahora parece no tener techo. Aquí tres libros que lo ayudarán a ingresar al mundo del popular Ubuntu.

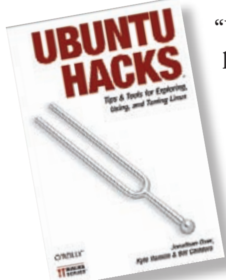
Ubuntu 7.10 *(PC Edition)*



Contiene un set completo de aplicaciones para desktop, laptops y servidores, además del Office, Web browser, e-mail para las necesidades diarias, mensajería instantánea, edición de imagen y varias herramientas para acceder y administrar los archivos multimedia. Incluye un DVD con una clara explicación de cómo instalar Ubuntu en el desktop y en el servidor además de todos los software de soporte en una decena de lenguajes diferentes.

Ubuntu Hacks: Tips & Tools for Exploring, Using, and Tuning Linux *(Hacks)*

Escrito por Jonathan Oxer, Kyle Rankin y Bill Childers, “Ubuntu Hacks” es una colección de 100 tips y herramientas que lo ayudarán a mejorar la instalación, configuración y customización de Ubuntu. Por ejemplo aprenderá cómo instalar y probar Ubuntu Linux, cómo convertir a Ubuntu en un centro multimedia en donde grabar discos, mirar videos y escuchar música, entre otras muchas cosas.



“Ubuntu Hacks”, en los 10 capítulos que lo componen, le ahorrará mucho tiempo en intentar solucionar problemas básicos y lo hará quedar como un real experto en el tema. Pero si lo que más disfruta es del viaje y no del destino en sí, entonces este no es el libro adecuado para usted ya que encontrará inmediatamente la solución a los problemas.

Con este libro conocerá los tips y técnicas que todo usuario de Ubuntu Linux debe manejar, sin importar el nivel de conocimiento y experiencia que se tenga con este sistema operativo y sus aplicaciones.

Ubuntu Linux Bible

La Ubuntu Linux Bible es un libro que contiene cientos de tips, guías y técnicas sobre Ubuntu. Sus más de 900 páginas se dividen en cuatro grandes temas: Primeros pasos (todo sobre la instalación), Ubuntu para el usuario normal, Ubuntu para administradores y Configuración de servidores.

Los principales puntos desarrollados son:
- Administración para el desktop y las redes.
- Envío de e-mails, edición de textos e impresión.
- Cómo bajar música, mirar DVDs y jugar.
- Cómo utilizar Ubuntu en laptops, estar wireless o sincronizar con su PDA.
- Configurar la Web, mails, DNS, DHCP y otros servidores.
- Administrar grupos y asegurar su red.

¿Está seguro que nuestros competidores conocen su negocio?



Diferencie a la hora de elegir quién será su aliado para proteger sus Sistemas de Información

Nuestros servicios de Seguridad de la Información, involucran el ciclo completo de la seguridad y se encuentran diseñados de forma tal que puedan estar al alcance de cualquier Organización. Proyectos controlados en tiempo y presupuesto, acorde a normas internacionales y profesionales altamente calificados, hacen de **SICinformática** su mejor opción a la hora de pensar en su próximo proyecto de Seguridad.

Partner Estratégico:

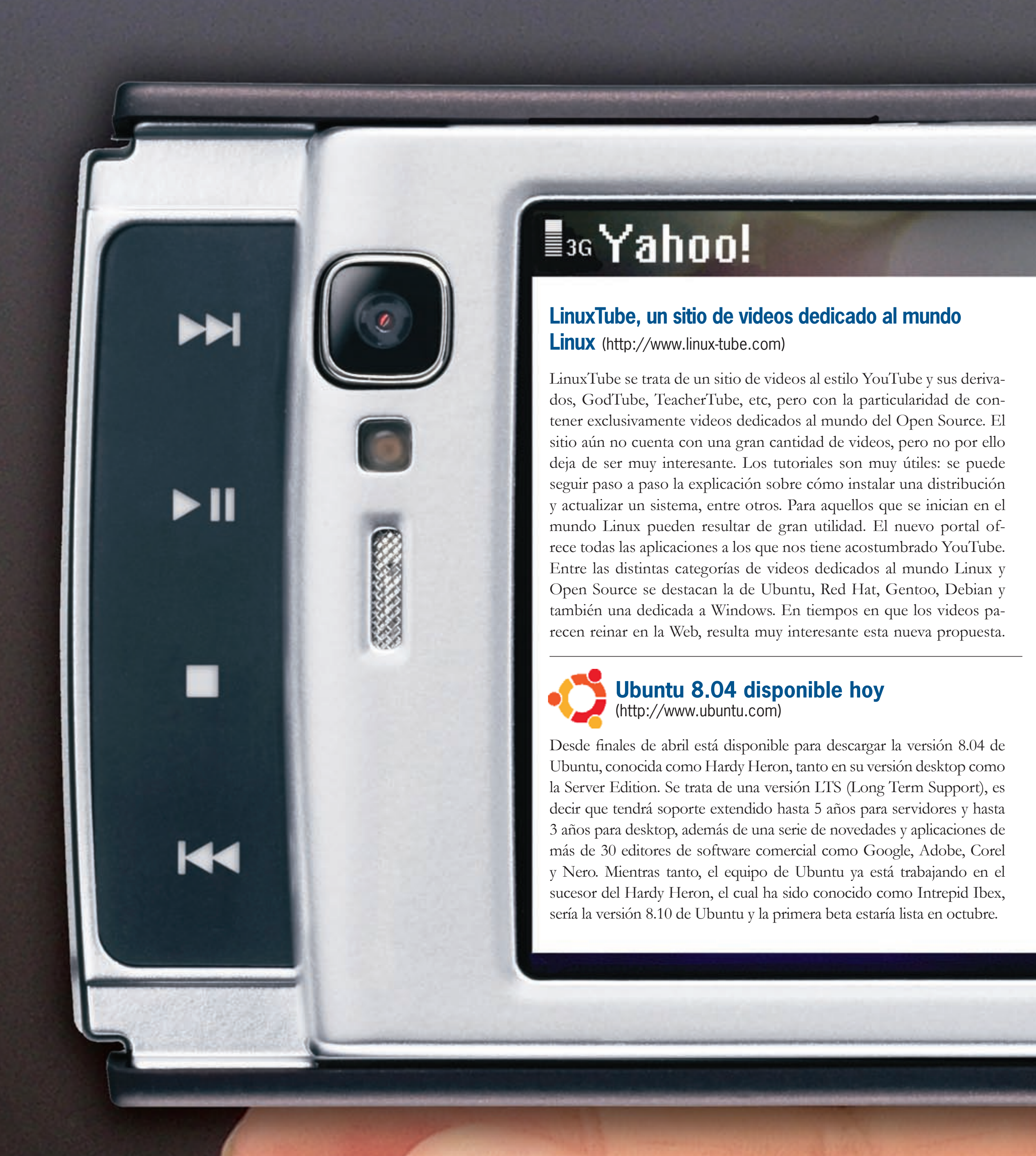


SIC
INFORMATICA
INFORMATION TECHNOLOGY & SECURITY SOLUTIONS

|Test de Intrusión | ISO 17799 | Consultoría | Capacitación | Anti-Fraude Online | Auditorías de Código | Seguridad Perimetral |

SICinformática S.R.L. | Tacuarí 237 Piso 9° Of. 98 (1071AAE) - Ciudad Autónoma de Bs.As., Argentina
Tel/Fax: (+54 11) 5218-4509 | www.sicinformatica.com.ar - info@sicinformatica.com.ar

NOTICIAS EN EL MUNDO



LinuxTube, un sitio de videos dedicado al mundo Linux (http://www.linux-tube.com)

LinuxTube se trata de un sitio de videos al estilo YouTube y sus derivados, GodTube, TeacherTube, etc, pero con la particularidad de contener exclusivamente videos dedicados al mundo del Open Source. El sitio aún no cuenta con una gran cantidad de videos, pero no por ello deja de ser muy interesante. Los tutoriales son muy útiles: se puede seguir paso a paso la explicación sobre cómo instalar una distribución y actualizar un sistema, entre otros. Para aquellos que se inician en el mundo Linux pueden resultar de gran utilidad. El nuevo portal ofrece todas las aplicaciones a los que nos tiene acostumbrado YouTube. Entre las distintas categorías de videos dedicados al mundo Linux y Open Source se destacan la de Ubuntu, Red Hat, Gentoo, Debian y también una dedicada a Windows. En tiempos en que los videos parecen reinar en la Web, resulta muy interesante esta nueva propuesta.

Ubuntu 8.04 disponible hoy (http://www.ubuntu.com)

Desde finales de abril está disponible para descargar la versión 8.04 de Ubuntu, conocida como Hardy Heron, tanto en su versión desktop como la Server Edition. Se trata de una versión LTS (Long Term Support), es decir que tendrá soporte extendido hasta 5 años para servidores y hasta 3 años para desktop, además de una serie de novedades y aplicaciones de más de 30 editores de software comercial como Google, Adobe, Corel y Nero. Mientras tanto, el equipo de Ubuntu ya está trabajando en el sucesor del Hardy Heron, el cual ha sido conocido como Intrepid Ibex, sería la versión 8.10 de Ubuntu y la primera beta estaría lista en octubre.

DEL SOFTWARE LIBRE



Llega Fedora 9 (http://docs.fedoraproject.org/)

Ya se encuentra disponible la versión previa de la versión 9 de Fedora, una de las distribuciones Linux más populares del mercado. Si bien el lanzamiento definitivo de Fedora 9 estaba previsto para fine de abril, se retrasará, por lo que se espera que para mediados de mayo esté en la calle. Mejoras en el hypervisor Xen, así como el apoyo a nuevos sistemas de ficheros, la inclusión de nuevas versiones del navegador Firefox y el entorno de escritorio KDE. Además incluye la nueva versión del entorno de escritorio GNOME, más precisamente la 2.22.

Nueva versión de MySQL

Sun Microsystem, quien compró hace unos meses MySQL en 1.000 millones de dólares, acaba de anunciar una nueva versión del sistema de gestión de base de datos. MySQL 5.1 es el nombre del nuevo software de código abierto y cuenta con varias mejoras en cuanto a la fiabilidad, velocidad y rendimiento. A partir del apoyo de una empresa como Sun, MySQL promete dar pelea en un mercado hasta ahora dominado por IBM y Oracle.

Nuevo líder para el proyecto Debian

Steve McIntyre ha sido elegido como nuevo líder del proyecto Debian, por medio de elecciones que se llevaron a cabo a mediados de abril. McIntyre, de 34 años de edad, es inglés y se desempeñaba como líder del equipo "debian-cd", que se encarga de generar los CDs y DVDs oficiales de la popular distribución de código abierto. El nuevo líder ocupará su cargo durante un año y viene a reemplazar a Sam Hocevar.

BREVES

Nuevo presidente de la OLPC

El proyecto One Laptop Per Child tiene ya a su nuevo Presidente, tras la renuncia al cargo del su principal mentor y fundador Nicholas Negroponte, quien no obstante continuará participando en las decisiones estratégicas y en la promoción. Se trata de Charles Kane quien hasta ahora se desempeñaba como Director Financiero.

Tras la incontable cantidad de problemas que la organización debió enfrentar en los últimos tiempos, Negroponte decidió retirarse de la presidencia afirmando que la Organización necesitaba ser conducida comercialmente a la manera de Microsoft, lo que generó una gran polémica en la comunidad Open Source. En los últimos meses el proyecto educativo ha perdido a tres de cinco de sus máximos responsables e impulsores y no ha encontrado la forma de hacer realidad su propuesta de llevar al ámbito educativo portátiles de 100 dólares, ya que hasta el momento las XO no se consiguen por menos de 188 dólares. Además se enfrentan a una competencia cada vez más feroz en el mercado, donde gigantes de la talla de Intel, Asus, HP y Dell han lanzado sus propias alternativas portátiles y de bajo costo. ●

Intel ya comercializó más de 10 millones de procesadores de cuatro núcleos

Según dio a conocer CNET, Intel ya ha superado los 10 millones de procesadores de cuatro núcleos vendidos, incluyendo más de 3.5 millones en el primer trimestre de 2008.

Esa impresionante cifra refleja que la industria ha recibido con los brazos abiertos a los procesadores de 45 nanómetros, en especial por el menor consumo de energía que estos posibilitan. Sin embargo el otro gran jugador del mercado de los microprocesadores, AMD, ya prepara su desembarco a gran escala en el segmento de los cuatro núcleos. A pesar de las dificultades financieras que enfrenta y de las fallas que presentaron los primeros procesadores Barcelona lanzados al mercado, la compañía dará pelea basándose en las ventajas de sus cuatro núcleos nativos. Los procesadores de cuatro núcleos actuales de Intel son realmente dos procesadores de dos núcleos en un encapsulado mientras que los cuatro núcleos de AMD son nativos porque incluyen los cuatro núcleos en una sola oblea. ●

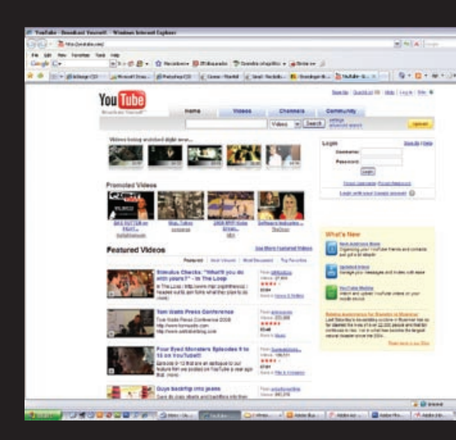
La Mini-Note de HP

Con el fin de ayudar a las escuelas a ofrecer computadoras económicas a todos los alumnos, HP presentó una minicomputadora portátil totalmente funcional a un precio inicial de menos de $500 dólares.

Diseñada para el mercado educativo, la HP 2133 Mini-Note PC es lo bastante flexible para que se utilice en diferentes ámbitos: pesa 1.3 kilogramos, tiene una pantalla amplia WXGA de 8.9 pulgadas en diagonal, teclado completo fácil de utilizar (QWERTY) y touchpad e incluye una suite de capacidades inalámbricas, multimedia y de seguridad para permitir a los estudiantes aprender dondequiera que vayan, entre otras muchas características. ●

Los 5 años de YouTube

El 28 de abril de 2003, Steve Jobs anunció el lanzamiento de la tienda de música digital, iTunes, con una oferta inicial de 200.000 canciones. Cinco años más tarde iTunes ofrece un catalogo de más de 6 millones de temas y se encuentra consolidado como líder absoluto en el atractivo mercado de las descargas online. Aquel lanzamiento sorprendió a muchos, ya que nadie esperaba que un fabricante de computadoras se lanzara al incipiente mercado de la comercialización de música digital. Sin embargo una vez más Steve Jobs y Apple han demostrado que posee una gran visión de negocios. iTunes tiene más del 70 por ciento de la cuota de mercado y suma más de 4.000 millones de canciones comercializadas.



No obstante, a futuro le esperan muchos desafíos a la tienda de Apple. El más duro al parecer es el del uso del DRM, ya que otros sitios como MySpace y en base a acuerdos con las discográficas han comenzado a ofrecer descargas sin el sistema anticopia.

Humor *por Severi*





PRÓXIMAMENTE
www.MEJOR
LAPTOP.com
Todo lo que querés saber
sobre laptops y
dispositivos móviles
que están revolucionando el mundo.
// Reviews
// Cámaras
// Tips and How To
// Videos
// Guia de compras
// Celulares
EP


like.no.other™
SONY
Sony recomienda Windows Vista® Home Premium.